UNIVERSIDADE ABERTA

Mestrado em Contabilidade e Auditoria

A certificação do relatório de controlo interno
Impacto do *outsourcing* de Tecnologias de Informação no risco de auditoria

João Manuel Laranjeiro de Almeida

Orientador: Dr. João Oliveira Rodrigues

Coimbra, Junho de 2008

I. Resumo

Com a evolução que se tem verificado na área das TI, é actualmente inconcebível qualquer organização não recorrer a meios informáticos para o processamento de dados.

Paralelamente a este panorama de evolução, verificam-se ainda duas tendências que importa salientar, o crescente recurso a *outsourcing* de TI pelas organizações e as novas exigências no que respeita ao SCI e ao seu relato. Neste ultimo caso, uma das principais exigências no que respeita ao SCI consiste na obrigação de relato sobre a eficácia do SCI presente na organização e a sua subsequente certificação pelos revisores/auditores independentes.

Neste contexto, é hoje evidente que os revisores/auditores, têm de enfrentar novas dificuldades no exercício da sua profissão, sendo a certificação do relatório da eficácia do SCI uma delas. Para essa certificação, o revisor/auditor terá então de avaliar o risco de auditoria, tendo em conta as condicionantes acima identificadas, relacionadas com o *outsourcing.*

Neste trabalho, pretende-se fundamentalmente evidenciar a existência de um acréscimo do risco de auditoria por força do recurso ao *outsourcing* de TI.

Para a realização deste trabalho foi efectuado um inquérito aos ROC, inscritos na OROC. Dos ROC consultados, obteve-se um total de 21 respostas. Apesar do diminuto número de respostas obtidas, o questionário foi tratado sob o ponto de vista descritivo e ainda sob a forma de testes de hipóteses.

Como resultado desse tratamento, verificamos que os factores PEST influenciam as características de informação segura e que a não validação dessas características influenciam tanto o risco de controlo como o risco de auditoria. Dessa forma, estes factores têm uma influência no julgamento que o auditor faz dos riscos de controlo e inerente. Face a estas conclusões, podemos afirmar que os factores PEST e, consequentemente, o *outsourcing* influenciam moderadamente o risco de auditoria. O trabalho conclui-se, com a evidência que o recurso a *outsourcing* de TI influenciará de forma importante o julgamento do risco de auditoria pelo auditor para efeitos de emissão de opinião sobre o relato do SCI inserido nas demonstrações financeiras.

II. Abstract

Face to the evolution in the IT area, actually any organization can't work without IT for the data processing.

In parallel to this view of evolution, there happen still two tendencies in what it imports to point out, the growing resource to IT outsourcing for the organizations and the new demand about internal control and his report. In this last case, one of the principal point respect to the management assessment of the effectiveness of internal control and the independent auditor attest to this report.

In this context, it is today obvious that the auditors will face new difficulties in their work, being the certification of the report of the effectiveness of internal control one of them. To form an opinion the auditor has to value the audit risk.

In this study, we intend to show up fundamentally the increase of the audit risk that result of the outsourcing IT.

For the realization of this study an inquiry was effectuated to the ROC registered in the OROC. We obtain a total of 21 answers of the consulted ROC. In spite of the tiny number of obtained answers, we study the questionnaire with descriptive statistic and hypotheses tests.

As result of this work, we check that the factors PEST influence the fundamental characteristics of safe information and that it not validation of these characteristics is influenced by both the risk of control and the risk of auditing. In this form, these factors have an influence in the judgment that the auditor does from the control risk and inherent risk. Face to these conclusions, we can affirm that the factors PEST and the outsourcing influence moderately the audit risk. The study ends, with the evidence that the resource to IT outsourcing will influence in the important form the auditor judgment of the audit risk in the assessment on the report of the Internal Control over financial reporting.

III. Lista de siglas

AICPA	*American Institute of Certified Public Accountants*
AS	*Auditing Standard*
COSO	*Committee of Sponsoring Organizations*
IFAC	*International Federation of Accountant*
ISACF	*Information Systems Audit and Control Foundation*
LSF	*Loi de sécurité financière*
NIR	Norma Internacional de Revisão
PCAOB	*Public Company Accounting Oversight Board*
PCGA	Princípios Contabilísticos Geralmente Aceites
PED	Processamento Electrónico de Dados
PEST	Factores sociológicos, políticos e legais, económicos, e tecnológicos
ROC	Revisores Oficiais de Contas
SAS	*Statement on Auditing Standards*
SCI	Sistema de Controlo Interno
SEC	*Securities and Exchange Commission*
SI	Sistemas de Informação
SOX	*Sarbanes-Oxley Act*
SROC	Sociedade de Revisores Oficiais de Contas
TI	Tecnologias de Informação

1. Introdução

Actualmente, é impensável qualquer organização, por muito que tenha uma dimensão diminuta, não recorrer a meios informáticos para os seus processamentos de dados.

Tem-se verificado, ainda, uma tendência para que essas mesmas organizações recorram a *outsourcing* nos mais diversos domínios, não sendo o domínio do processamento electrónico de dados excepção.

Uma recente lei, *Sarbanes-Oxley Act*, veio, de alguma forma, tentar dar resposta aos diversos problemas postos à luz do dia por conhecidos escândalos financeiros dos quais são exemplos os casos da Enron e, mais recentemente, da Parmalat. A referida lei prevê, na sua secção 404, que as Administrações relatem a eficácia do sistema de controlo interno e que os revisores/auditores independentes certifiquem esse relato.

Estas imposições levantam várias questões, as quais constituem a problemática a estudar neste trabalho, designadamente quando a organização está dependente de processamento electrónico de dados e recorre para o mesmo a *outsourcing*. Nesses casos, o risco de auditoria poderá aumentar por força desse *outsourcing*.

Das considerações feitas acima, propomos um estudo que permite realçar em relação à certificação do relatório do Sistema de Controlo Interno o impacto que o *outsourcing* de Tecnologias de Informação poderá ter no risco de auditoria, sendo nosso objectivo mostrar que esse mesmo risco aumenta quando a organização recorre ao *outsourcing* para as suas TI.

O presente estudo encontra-se dividido, resumidamente, em três partes.

Na primeira parte, faremos o enquadramento teórico da problemática que se pretende estudar, recorrendo para isso à diversa literatura existente tratando destas matérias. Nesta parte, analisaremos com maior pormenor a legislação mais recente, surgida como forma de respostas aos, já citados acima, escândalos financeiros, nomeadamente a *Sarbanes-Oxley Act*, e a *Loi de sécurité financière*. Da análise destes dois normativos, passamos à estruturação da problemática a estudar.

Como resultado da fixação do objecto do nosso estudo, surge a necessidade de análise de vários conceitos, intimamente ligados a este, nomeadamente: SCI, TI e PED,

risco de auditoria, e *outsourcing*. Cada um destes conceitos representará um capítulo próprio em que serão analisadas várias questões ligadas a este.

Para o estudo do conceito de SCI, analisaremos os conceitos apresentados por várias entidades normalizadoras, nomeadamente: *International Federation of Accountant*, com o estudo da Norma Internacional de Revisão nº 410 – Controlo interno, o IT *Governance Institute*, com o estudo do CobiT, o *Public Company Accounting Oversight Board*, com o estudo da *Auditing Standard* nº 2 – *An audit of internal control over financial reporting performed in conjunction with an audit of financials statements* e, por último, o *Committee of Sponsoring Organizations of the Treadway Commission* com a análise do COSO.

Na questão das TI e PED, verificaremos qual o conceito de controlo interno informático, subdividindo estes pelos conceitos relacionados de controlos de prevenção, controlos de correcção, e controlos de detecção.

Passaremos de seguida ao conceito de risco de auditoria, o qual também terá forçosamente de ser analisada através dos vários conceitos correlacionados, a saber: risco inerente, risco de controlo e, risco de detecção.

Por último, no que respeita aos conceitos, verificaremos o conceito de *outsourcing*. Como forma de melhor apreender este conceito, optamos por identificar numa primeira parte diferentes tipos de *outsourcing*. Tomamos esta opção de estudo com o intuito de apresentar a diversidade de opiniões que existem sobre esta matéria, ainda controversa, verificando uma multiplicidade de classificações, segundo os diversos estudiosos destas questões, as quais tentamos agrupar em cinco grupos, para melhor compreensão. Definido de forma mais clara qual o nosso entendimento sobre o *outsourcing*, analisamos então os riscos que poderiam decorrer do processo de *outsourcing*. Verificamos que a literatura sobre estas matérias associa os factores sociológicos, políticos e legais, económicos, e tecnológicos, a factores de risco incorridos com o *outsourcing*, pelo que procedemos à sua análise mais pormenorizada.

Num segundo tempo, elaboramos um parágrafo referente ao estudo empírico realizado, com base nos estudo teórico efectuado. Este ponto encontra-se subdividido em três grandes capítulos, tratando nomeadamente: a forma de abordagem do problema, a análise das respostas obtidas, e as conclusões a retirar do inquérito. No ponto tratando da forma de abordagem do problema, evidenciaremos a opção que tomamos de não questionar

directamente os respondentes, mas sim de apresentar diversos itens representativos das matérias a estudar, solicitando que sejam escolhidos apenas alguns. Quanto ao ponto tratando da análise efectuada às respostas obtidas, efectuaremos análises de dois tipos, nomeadamente: análise descritiva e testes de hipóteses. Com a realização destes dois parágrafos ser-nos-á então possível passar ao último ponto da segunda parte deste trabalho, onde teceremos as nossas conclusões sobre os resultados obtidos.

O nosso terceiro grande capítulo para este estudo respeita às conclusões que retiramos do estudo que efectuamos, agora de uma forma mais genérica. Por último, encontram-se evidenciadas as limitações e extensões que consideramos estarem presentes neste trabalho.

2. Enquadramento teórico / Revisão da literatura

2.1. Legislação

Como forma de resposta aos diversos problemas postos à luz do dia por diversos escândalos financeiros como o caso designadamente da Enron e da Parmalat, surgiu diversa legislação, a nível internacional (Hassid, 2005), entre as quais podemos citar a SOX e a *loi nº 2003-706, du 1er août 2003 de sécurité financière*. Esta legislação veio, de alguma forma, provocar alterações no panorama da auditoria (Rouse e al., 2004). Da sua análise conclui-se que as duas incluem globalmente os mesmos requisitos, perseguindo objectivos idênticos, e que podem ser resumidos ao facto de permitir a detecção atempada os riscos incorridos pelos investidores e prevenir a ocorrência de comportamentos fraudulentos por parte da administração, recorrendo para isso a obrigações de comunicação mais explícitas e ao agravamento das penas já existentes para esses casos, bem como à fixação de penas novas (Hassid, 2005).

2.1.1. A Sarbanes-Oxley Act

Esta legislação, com o objectivo de "proteger os investidores melhorando a exactidão e fiabilidade das divulgações das organizações tornando-as consistentes com a legislação e outros fins" (SOX, 2002), deverá contribuir para providenciar uma segurança razoável que relatos financeiros fraudulentos poderão ser prevenidos ou detectados atempadamente.

Para além de criar o PCAOB, a SOX fixou, ainda, a definição de regras para fomentar a necessária independência dos auditores, e a definição das responsabilidades das organizações. Foram ainda fixadas normas para permitir uma melhoria da informação financeira divulgada e definidos os crimes em que poderão incorrer os diversos intervenientes no processo de divulgação de informação financeira e da auditoria a que a mesma é sujeita.

Para o estudo que nos propomos aqui realizar, o nosso interesse incidirá, essencialmente, sobre duas secções, o *title III – Corporate* responsibility e o *title IV – Enhanced financial disclosures*, que tratam as duas de controlo interno.

A *sec. 302 – Corporate responsibility for financial reports*, define as responsabilidades da administração e dos responsáveis pelos serviços financeiros em relação ao relato financeiro. Dessa forma requer que o director geral e o director financeiro ou quaisquer outros elementos desempenhando as mesmas funções, para as sociedades cotadas em bolsa atestem, nos seus relatos financeiros anuais e trimestrais, entre outros requisitos, que os responsáveis pela sua elaboração e identificados como tal nas mesmas, são igualmente responsáveis pelo estabelecimento e manutenção do controlo interno. Estes deverão ainda atestar que o mesmo foi concebido de forma a garantir que o relato da informação financeira materialmente relevante divulgada aos utilizadores e às subsidiárias da organização tenha sido dado a conhecer a essa mesma administração por terceiros pertencentes à organização, com especial relevo para o período em que os relatórios periódicos são emitidos. Para um período máximo de 90 dias anteriores à data do relatório, deverá ter sido avaliado o SCI verificando a sua eficácia junto dos utilizadores desse, e devendo os responsáveis pela elaboração do relato financeiro apresentarem as suas conclusões acerca da sua avaliação nesse período, concluindo sobre a eficácia do SCI (SOX, 2002). Porém, as exigências feitas aos administradores e responsáveis financeiros

no que respeita aos SCI não são, nessa secção, passíveis de avaliação externa quando à sua fiabilidade.

Para suprir esta lacuna da *sec. 302*, teremos de analisar a *sec.404 - Management assessment of internal controls.*

A *sec. 404* da SOX veio tornar obrigatória, para todas as empresas registadas junto da *Securities and Exchange Commission*, a elaboração de um relatório sobre o SCI inerente ao relato financeiro, da responsabilidade da administração, devendo a SEC fixar normas nesse sentido. Paralelamente, requer que sejam adoptadas normas pelo PCAOB com vista à certificação desse mesmo relatório pelos auditores independentes dessas organizações (SOX, 2002). Em 15 de Fevereiro de 2005, o PCAOB emitiu a *AS nº 2 – An audit of internal control over financial reporting performed in conjunction with an audit of financial statements*, de forma a dar cumprimento ao previsto nesta secção da SOX. Nesta norma, é fixada a obrigatoriedade dos órgãos de gestão das organizações sujeitas à normalização da SEC incluírem no seu relatório anual o seu julgamento no que concerne à eficácia do controlo interno inerente ao relato financeiro (PCAOB, 2005), constituindo então uma obrigação para a administração. Da mesma forma, são definidas as normas no que respeita às obrigações dos auditores independentes incumbidos da auditoria a essas organizações. Estes deverão, em relação ao julgamento da administração, emitir a sua opinião, certificando o julgamento da administração incluído no relato financeiro (PCAOB, 2005).

A certificação emitida pelo auditor, de forma a dar cumprimento ao preconizado pela *sec. 404 (b)* deverá assentar sobre uma base sólida, resultante de um correcto planeamento e subsequente auditoria de forma a obter evidência sobre as suas conclusões e proporcionar uma segurança razoável de que o SCI inerente ao relato financeiro, presente na organização, é efectivo, em todos os seus aspectos materialmente relevantes, à data especificada pela administração (PCAOB, 2005).

2.1.2. *Loi de sécurité financière*

A LSF, composta por quatro títulos principais, nomeadamente: *modernisation des autorités de controle, sécurité des épargnants et des assurés, modernisation du controle legal des comptes et transparence*, e *dispositions relatives à l'outre-Mer*. Esta lei veio

afectar o direito dos seguros, financeiro, bancário, e contabilístico, para além de serem tomadas numerosas medidas com impacto nas organizações (SGDM, ???). Para o nosso estudo, iremos interessar-nos pelas implicações desta lei no direito das sociedades essencialmente previsto no seu título III.

No campo da melhoria da transparência das sociedades, a LSF preocupa-se com a informação prestada aos investidores, com o objectivo de lhes possibilitar um melhor acompanhamento, ao longo de todo o exercício, da gestão da empresa (SGDM, ???). Para tal, salientamos nos parágrafos seguintes duas medidas apontadas pela LSF.

A administração da organização, conforme previsto no artigo 117 do capítulo II, que modifica o artigo L.225-37 do *code de commerce*, passa a ter que relatar, conjuntamente com o relato anual, as condições em que foram desempenhadas as suas funções e como as mesmas foram organizadas, bem como o SCI presente na organização. Está ainda previsto neste artigo, especificamente, que a administração indique, quando aplicável, em que medida os poderes do director geral foram limitados. Neste mesmo artigo da LSF é modificado o artigo L.225-68 do *code de commerce* prevendo que o presidente do comité de auditoria da organização relate à assembleia-geral da organização, também ele, as condições em que foram desempenhadas as suas funções e como as mesmas foram organizadas, bem como o SCI presente na organização. Este relatório deverá integrar o relato anual destinado aos utilizadores da informação financeira.

Paralelamente à informação mencionada no parágrafo acima, está previsto na LSF, no artigo 120 do capítulo III, o qual modifica o artigo 225-235 do *code de commerce*, que um auditor independente apresente, conjuntamente com o seu relatório, as suas conclusões sobre o relato emitido, conforme os casos, pela administração ou pelo comité de auditoria, no que respeita ao SCI inerente ao relato financeiro.

2.2. A problemática a estudar

Da análise que efectuamos à literatura existente sobre a recente legislação acima citada, detectamos a existência de uma problemática, ainda não estudada, referente à interligação de vários conceitos presentes, ainda que de forma implícita, tanto na SOX como na LSF, as quais passaremos a designar, doravante, e tendo em conta o facto de,

como concluímos, as duas poderem ser consideradas, ainda que globalmente, equivalentes, por legislação. Como tal, passaremos de seguida à explicitação desta problemática e do interesse que a mesma nos despertou, motivando-nos para a realização deste estudo.

As TI são consideradas, por alguns autores (Cannon, 2004; Lijima, 2004) cruciais face às exigências feitas pela SOX. Estes reconhecem ainda que, muitas vezes, os responsáveis por esses departamentos não estarão suficientemente sensibilizados para as implicações destas no sistema de controlo interno da entidade.

Considera-se que as TI fazem parte integrante das transacções financeiras, estando intimamente ligadas a todo o processo de relato financeiro (ISACF, 2003), podendo-se portanto concluir quanto à importância das TI em relação ao SCI inerente ao relato financeiro. (ISACF, 2003)

O recurso a TI por parte das mais diversas organizações altera as "considerações do risco inerente e do risco de controlo pelas quais o revisor/auditor chega à avaliação do risco (IFAC, NIR 401).

Acresce ainda o facto de, por vezes, os controlos identificados pela gerência poderem englobar as TI (ERNST & YOUNG LLP, 2002). O auditor deve então "obter um conhecimento suficiente dos sistemas contabilísticos e de controlo interno afectados pelo ambiente de SIC" (IFAC; NIR 401) e "determinar o efeito do ambiente de SIC na avaliação do nível do risco global" (IFAC, NIR 401).

Porém, ao falarmos de TI, actualmente, não podemos deixar de interligar estas com o recurso, cada vez mais frequente, ao *outsourcing*, acrescentando este, uma nova dimensão a questão cultural e de controlo que poderá ser examinada separadamente (Cannon, 2004).

Como vimos nos pontos acima, a legislação prevê a emissão de um relatório sobre a eficácia do SCI inerente ao relato financeiro, bem como a certificação desse relatório e desse SCI, por parte de um auditor independente. Essas exigências vêem, então, acrescentar uma nova dimensão aos estudos acima evidenciados

Da revisão de literatura tratando de temas como as TI, o *outsourcing* de TI, e o relato de controlo interno, verificamos que não existe uma conjugação dessas três questões o que, entendemos, poderá acrescentar uma nova visão a estes temas.

Detectamos a existência de estudos tratando das problemáticas inerentes às TI mas não tratando essas questões introduzindo a variante do *outsourcing*. De entre esses estudos,

existem alguns, essencialmente relacionados com a secção 404 da SOX, que acrescentam, por força do estudo dessa secção, a problemática do relato do sistema de controlo interno da entidade em ambiente PED. Os ditos estudos, não analisam, no entanto, o impacto que o *outsourcing* poderá vir a ter no sistema de controlo interno da entidade e, desde logo, no relato desse mesmo sistema.

Outros estudos existem, no que respeita à dependência existente entre o *outsourcing* de TI e o risco de controlo. Esta questão, que parece assemelhar-se à nossa escolha segue, ao contrário do que é nossa intenção, uma visão assente na auditoria interna não na auditoria externa. A certificação do relatório de controlo interno, emitido pela gerência das sociedades, será da responsabilidade de auditores externos, nunca de auditores internos, fomentando a necessária independência dos auditores externos. Dessa forma, entendemos que o estudo assente em conceitos destinados à auditoria externa poderá permitir evidenciar novas variantes destas questões.

2.3. Conceitos

Com vista à definição de um quadro conceptual a seguir para este estudo, e tendo em conta as conclusões a que chegamos no parágrafo acima, começaremos pela análise dos conceitos de maior importância para este tema, e que se encontram evidenciados na diversa literatura estudada sobre este tema. Como tal, elegemos como conceitos a analisar os seguintes: SCI, TI e PED, Risco de Auditoria, e *outsourcing*.

Comecemos esta análise com o conceito de SCI.

2.3.1. Sistema de controlo interno

Para verificar qual o conceito de SCI que iremos utilizar tendo em conta o estudo que nos propomos realizar, entendemos analisar a normalização específica existente, designadamente: NIR nº 410 – Controlo interno; CoBit[1]; e *AS nº 2 – An audit of internal*

[1] *Standard* mais utilizado no trabalho de auditoria segundo estudo realizado em 1998 pelo ISACA – *Benchmark* sobre a profissão de auditores de sistemas de informação.

control over financial reporting performed in conjunction with an audit of financial statements. A escolha desta normalização derivou directamente do tema que nos propomos estudar. Este tema, tratando do relato do SCI inerente ao relato financeiro, leva-nos a análise de normalização emanada por organismos normalizador para a auditoria financeira, para os quais elegemos a NIR nº 410. Porém, a problemática que aqui fixamos, analisa mais concretamente o impacto que as TI poderão ter na avaliação desse SCI inerente ao relato financeiro, como tal, pareceu-nos adequada a análise de normalização emanada por organizamos normalizadores para a auditoria informática, facto que nos levou a eleger a análise do CobiT. Por último, não poderíamos deixar de analisar o conceito de SCI previsto na AS nº 2, derivado ao facto de esta ser emanada pelo organizamos normalizador criado especificamente para responder a esta nova exigência de relatar o SCI inerente ao relato financeiro, o PCAOB. Esperamos que esta análise permita evidenciar algumas diferenças entre estes conceitos que nos poderão ser úteis para a prossecução do nosso estudo e fixar qual o conceito de SCI que iremos utilizar ao longo do mesmo.

2.3.1.1. NIR nº 410 – Controlo Interno

A NIR 410 define SCI como evidenciamos de seguida:

"o termo "sistema de controlo interno" significa todas as políticas e procedimentos (controlos internos) adoptados pela gerência de uma entidade para contribuir para a obtenção do objectivo da gerência de assegurar, tanto quanto praticável, a condução ordenada e eficiente do seu negócio, incluindo a aderência às políticas de gestão, a salvaguarda de activos, a prevenção e detecção de fraude e erros, o rigor e a plenitude dos registos contabilísticos, e a preparação tempestiva de informação financeira credível." (IFAC, NIR 410: 4).

Da análise mais aprofundada desta definição verificamos que a noção de controlo interno está intimamente ligada aos objectivos que se pretendem atingir através da sua implementação. No caso desta norma, os objectivos perseguidos confundem-se com os objectivos da gerência, pressupondo-se que estes estarão relacionados essencialmente com a eficiência do negócio. Para esta norma, para que esta eficiência possa ser atingida terão

de se ter em atenção aspectos como a salvaguarda dos activos da organização, a existência ou não de fraudes e erros, os registos contabilísticos existentes e que servirão para a preparação da informação credível.

Concluindo, podemos afirmar que a noção de SCI prevista pela NIR nº 410 está intimamente ligada ao desempenho financeiro da organização, devendo da sua implementação e utilização resultar informação financeira credível. A preocupação da salvaguarda de todos estes aspectos não deverá porém ser impeditiva da divulgação atempada dessa mesma informação financeira.

2.3.1.2. CobiT

O CobiT não define directamente a noção de SCI, mas sim a noção de controlo interno, a qual evidenciamos de seguida:

"as políticas, procedimentos, práticas e estruturas da organização desenhadas de forma a proporcionar uma segurança razoável que os objectivos do negócio serão atingidos e que factos não desejáveis serão prevenidos ou detectados e corrigidos."[2] (ISACF, 2002(b)).

Numa primeira abordagem a definição de controlo interno dada pelo CobiT parece ser mais concisa, porém uma abordagem mais aprofundada permite verificar que esta levanta aspectos, não previstos na NIR nº 410 analisada acima mas não menos importantes.

Também aqui a preocupação principal do controlo interno está relacionada com os objectivos do negócio, logo os objectivos seguidos pela gerência das organizações. Porém, para se atingir tais objectivos, entende-se que será necessário que existam, para além de políticas e procedimentos adequados, práticas e estruturas adequadas. Neste caso, entende-se que da própria estrutura da organização poderá resultar, ou não, um adequado sistema de controlo interno. Esta questão parece-nos de facto pertinente, visto que não se pode esquecer que as políticas e procedimentos a implementar deverão ter em conta questões como a especificidade e a estrutura da organização em que as mesmas se podem

[2] Tradução nossa.

implementar. Esta norma quer com isto alertar para a especificidade subjacente ao controlo interno de cada organização. A adopção de um sistema de controlo interno, comprovadamente eficiente, presente numa determinada organização, com uma determinada estrutura, poderá não ser eficiente quando adoptado a uma organização com uma estrutura diferente.

Esta definição não foca o seu objectivo principal na informação financeira emanada pela organização, mas sim na totalidade dos objectivos do negócio. Este facto é aliás, perfeitamente aceitável, tendo em conta que estamos perante uma norma emanada por organismos ligados às tecnologias de informação ao contrário da NIR nº 410 emanada por um organismo ligado à auditoria.

Por último, verificamos que esta norma avança com mais uma questão no que respeita a erros ou fraudes, aos quais chama de forma mais abrangente "factos não desejáveis". Para além da questão da prevenção e detecção desses factos, entende ainda que é necessário que o controlo interno preveja a sua correcção no caso em que estes venham a ocorrer. É possível então definir vários níveis de controlo interno, classificando-os de várias formas, conforme evidenciamos no ponto seguinte.

2.3.1.2.1. A classificação dos níveis de controlo interno

2.3.1.2.1.1. Controlo interno de prevenção

Este controlo deve garantir que são tomadas as condições necessárias para que não venham a ocorrer erros, incidindo sobre as causas de risco, tendo como objectivo a diminuição da frequência com que as mesmas se manifestam.

2.3.1.2.1.2. Controlo interno de correcção

Estes controlos têm uma finalidade essencial de investigação, isto é, permitem que se identifiquem as causas de risco e, consequentemente, que se tomem as devidas medidas

correctivas para que as mesmas deixem de existir ou que, pelo menos, as mesmas sejam reduzidas a um nível aceitável.

2.3.1.2.1.3. Controlo interno de detecção

O controlo interno de detecção surge devido às necessidades evidenciadas pelos controlos de correcção. A correcção das causas de risco detectadas pelo controlo correctivo pode resultar difícil e ineficiente, pelo que será necessária a implementação dos controlos de detecção. Espera-se que, neste nível de controlo, seja possível a detecção, com a maior brevidade possível, de erros e de potenciais causas de risco. Este nível de controlo deverá permitir validar a eficiência do controlo interno de prevenção. Se o controlo interno de prevenção for eficiente, então deverá resultar do controlo de detecção a inexistência de erros ou de potenciais causas de risco.

2.3.1.3. AS nº 2 – *An Audit of internal control over financial reporting performed in conjunction with an audit of financial statements*

A AS nº 2 define o controlo interno com ênfase no relato financeiro, como transcrevemos de seguida:

"Um processo desenhado por, ou sob a supervisão da direcção da organização e do responsável máximo financeiro ou por pessoas desempenhando funções similares, e implementado pelo conselho de administração, pela gestão e pelo restante pessoal, de forma a proporcionar uma segurança razoável no que respeita à fiabilidade do relato financeiro e à preparação das demonstrações financeiras destinadas ao exterior em conformidade com os PCGA incluindo estas políticas e procedimentos que:

- respeitem à manutenção de registos que, razoavelmente, com precisão e suficientemente, reflectem as transacções e as disposições dos activos da organização;

- proporcionem segurança razoável que as transacções foram registadas convenientemente para permitir a elaboração das demonstrações financeiras em

conformidade com os PCGA e que os recebimentos e as despesas da organização foram efectuados em conformidade com autorização da gestão e direcção da organização; e

- proporcionem uma segurança razoável respeitante à prevenção ou detecção atempada de aquisições não autorizadas, uso ou disposição dos activos da organização que poderão ter um efeito materialmente relevante nas demonstrações financeiras."[3] (PCAOB, 2004).

Um dos aspectos mais visíveis desta definição prende-se com o facto de esta definir, ao invés do que acontecia com as duas definições vistas anteriormente, a responsabilidade pela concepção do SCI. A NIR nº 410 apenas refere que o SCI deverá ser adoptado pela gerência enquanto o CobiT nada refere quanto a eventuais responsabilidades pela concepção desse sistema. Esse preciosismo, embora possa parecer insignificante e óbvio toma, em nosso entender, a sua maior importância quando nos confrontamos com um SCI inerente ao relato financeiro mas com base em dados obtidos através do recurso a *outsourcing*[4].

Define-se, de forma clara, quem são os órgãos da organização responsáveis: direcção da organização e responsável máximo financeiro, podendo este último ser substituído por pessoas desempenhando funções similares. Esta responsabilização é perfeitamente justificada, tendo em conta que estamos a falar de SCI inerente ao relato financeiro, sendo o objectivo desse SCI a obtenção de relato financeiro fiável, sendo também neste caso, a administração responsável pela sua preparação, conforme podemos verificar pela leitura da SAS nº 1 – *Responsibilities and functions of the independent auditor*[5].

[3] Tradução nossa.

[4] Devemos entender neste ponto *outsourcing* em sentido lato, ou seja, *outsourcing* de qualquer serviço e não apenas o *outsourcing* de sistemas de informação que pretendemos analisar neste estudo. De facto, qualquer que seja a natureza do *outsourcing* realizado, terá de possuir sempre um SCI.

[5] A normalização portuguesa prevê a responsabilização do órgão de gestão pela preparação das demonstrações financeiras, no parágrafo nº 20 das Normas Técnicas de Revisão / Auditoria.

2.3.1.4. Conceito de controlo interno a utilizar no estudo

As definições que estudamos acima resultam, como vimos, de normalização vigente tanto para a auditoria financeira como para a auditoria de sistemas de informação. O último conceito, previsto pela AS nº2, seria o conceito que, logicamente, se deveria adequar melhor ao nosso estudo, visto estar directamente relacionado com o tema deste. Porém, ao efectuar a sua análise detectamos a existência de dois pontos que nos pareceram relevantes para a fixação do SCI a utilizar neste estudo os quais passamos a referir.

A AS nº 2 prevê, nomeadamente nos seus pontos 13 e 14 que os julgamentos efectuados pelo órgão de gestão no que concerne à eficiência do SCI inerente ao relato financeiro se apoiem num quadro conceptual de controlo reconhecido, fixando as condições em que o mesmo se poderá considerar corresponder a esses parâmetros, nomeadamente: estar isento de quaisquer preconceitos, permitir avaliar qualitativamente e quantitativamente de forma razoável o SCI inerente ao relato financeiro de uma organização, ser completo o suficiente não permitindo que factos relevantes que possam alterar as conclusões acerca da efectividade do SCI inerente ao relato financeiro não sejam detectados, e ser relevante para uma avaliação do SCI inerente ao relato financeiro. Refere-se, ainda, no ponto seguinte, que para os Estados Unidos, se pode considerar que o quadro conceptual do COSO, cumpre com os requisitos fixados por esta norma. Como tal, a AS nº2 seguirá o quadro conceptual do COSO. Tendo em conta este ponto, vejamos então, de seguida, o conceito de SCI dado pelo COSO.

2.3.1.4.5. O COSO

O quadro conceptual emanado pelo COSO identifica cinco componentes inter-relacionadas, para o controlo interno, nomeadamente: ambiente de controlo, avaliação do risco, actividades de controlo, informação e comunicação, e acompanhamento. Vejamos de seguida o que representam estas componentes:

- Ambiente de controlo: este representa a base de todas as outras componentes de controlo interno. Prende-se com a necessidade de existir uma consciencialização geral da necessidade de um bom SCI na organização.

- Avaliação do risco: esta avaliação passa pela necessidade de se definir quais os objectivos que se pretendem atingir. Após a definição destes, será então possível proceder

a uma identificação dos riscos existentes, procedendo-se posteriormente à sua análise de forma a estudar soluções para os gerir da melhor forma possível.

- Actividades de controlo: um bom SCI não pode depender meramente da identificação dos riscos e da sua gestão como vimos no ponto acima. Há ainda que definir formas de controlar que as políticas fixadas pelos órgãos competentes para gerir o risco são de facto cumpridas.

- Informação e comunicação: o pessoal deve, a todo o momento, ter acesso a sistemas de informação e comunicação, que lhe permita o acesso à informação.

- Acompanhamento: no final da pirâmide das componentes do controlo interno, surge o acompanhamento. Porém, este é desenvolvido ao longo de todo o processo de implementação e gestão do SCI. Os procedimentos de controlo implementados deverão ser acompanhados com regularidade de forma a se poderem efectuar as modificações necessárias.

Tendo em conta estes dados, optamos por utilizar, ao longo do nosso estudo, as componentes do controlo interno identificadas no quadro conceptual do COSO. Dessa forma, procuraremos identificar qual a percepção dos auditores em relação a esses níveis de controlo interno, definindo qual o nível a partir do qual os mesmos consideram que existe efectivamente um SCI eficaz.

2.3.2. Tecnologias de informação e processamento electrónico de dados

Actualmente, face à importância da informação, é impensável qualquer organização, ainda que tenha uma dimensão diminuta, não recorrer a TI, porém, não se deve cometer o erro de associar a informática às TI, sendo as TI muito mais do que apenas computadores ou mesmo utilização de meios informáticos para o processamento electrónico de dados. Resumindo, de uma forma simples, podemos exemplificar essa diferença da seguinte forma: todos os meios informáticos para processamento electrónico de dados representam TI mas nem todas as TI representam meios informáticos para processamento electrónico de dados.

Por TI, podemos entender todo e qualquer recurso, não humano, que permita recolher, processar, armazenar, tratar, e distribuir informação.

Tendo em conta a complexidade deste conceito, entendemos limitar o nosso estudo às TI directamente relacionadas com o processamento electrónico de dados, ou seja, às TI relacionadas com a utilização de meios informáticos pela empresa e, neste caso específico, para as quais a empresa recorra a *outsourcing*.

Com o âmbito do nosso estudo definido no que respeita às TI, e seguindo a nossa ideia do ponto anterior, podemos então passar à análise do controlo interno inerente a essas mesmas TI.

2.3.2.1. O controlo interno informático

O controlo interno informático tem como finalidade principal a verificação de todas as actividades desenvolvidas pelos SI. Como tal, esse controlo testa o cumprimento dos procedimentos e normas definidos, em princípio pela gestão de topo e/ou pela direcção informática.

Este conceito de controlo interno informático pode porém ser interpretado de diferentes formas consoante estejamos a falar de auditoria interna ou de auditoria externa. No caso da auditoria interna, a empresa é vista como um sistema, sendo, desde logo, o âmbito do controlo interno muito mais abrangente. Já no caso da auditoria externa, frequentemente as preocupações com o SCI presente ao nível informático prendem-se mais com as áreas funcionais apresentando maiores riscos em termos financeiros. Esta distinção levanta uma problemática para este estudo em que pretendemos avaliar, ainda neste ponto, qual o impacto no risco de auditoria do recurso a TI, comprovando que, conforme é referido por exemplo na NIR nº 401 – A revisão/auditoria num ambiente de sistema de informação computorizado, "a complexidade das aplicações específicas (…) podem aumentar o risco". Vejamos de seguida quais os aspectos de controlo interno informático nos quais podemos apoiar a nossa análise.

O controlo interno informático pode ser decomposto em traços gerais, por: preventivo, correctivo, e de detecção. De seguida analisaremos com mais profundidade o que se entende por cada uma dessas subdivisões.

2.3.2.1.1 Os controlos de prevenção

Estes controlos, também conhecidos por controlos dissuasores, têm como finalidade o estabelecimento de condições que permitam a diminuição da ocorrência de causas de erros estabelecendo, dessa forma, as condições necessárias para a não ocorrência de erros.

2.3.2.1.2. Os controlos de correcção

Estes controlos ajudam a investigar quais as causas de erros e, dessa forma, permitem que sejam aplicadas medidas correctivas a essas causas.

2.3.2.1.3. Os controlos de detecção

Estes controlos têm como principal objectivo a detecção rápida das causas de risco e de erros. São frequentemente considerados os de maior importância para o auditor. Nestes controlos de detecção podemos evidenciar os controlos de supervisão. Estes controlos permitem à gestão tomar conhecimento das eventuais situações de risco existentes, sendo estas posteriormente acompanhadas de forma a permitir a tomada de decisão sob qual a melhor estratégia para conseguir atingir os objectivos fixados pela empresa. Tendo em conta os objectivos perseguidos pelos controlos de supervisão (controlar a evolução empresarial de forma alcançar os objectivos fixados) podemos então concluir que estes proporcionam à direcção e, consequentemente, ao auditor, um maior nível de confiança na informação financeira transmitida, considerando-se uma maior fiabilidade da mesma quanto mais eficazes forem os controlos de supervisão. Podemos agrupar os controlos de supervisão em três tipos: controlos de aplicações, controlos de tecnologias de informação, e controlos de utilizadores. Analisemos abaixo estes controlos separadamente.

Os controlos de aplicações consistem em diversas rotinas que deverão incidir sobre a própria aplicação, as quais poderão ser previamente programadas para serem executadas de forma automática num determinado momento. Porém, e com o intuito de garantir um maior nível de controlo, deverão ainda existir rotinas executadas manualmente e

aleatoriamente no tempo de forma a prevenir a existência de possíveis fraudes. Estas rotinas deverão ter em conta a especificidade da aplicação que se pretende controlar, podendo-se dizer de forma resumida que as mesmas permitirão a avaliação dos dados em três momentos distintos: recolha dos dados, processamento dos dados, e saída dos dados. Esta avaliação terá como objectivo verificar que os dados são recolhidos de forma correcta, tanto no que respeita à quantidade de dados recolhidos como à sua exactidão, que o seu processamento é feito de forma adequada, prevenindo e detectando eventuais erros de entradas, de processamento, etc, e que os dados retirados da aplicação no final são exactos, concordantes com as entradas e apenas acessível a utilizadores autorizados.

Os controlos da tecnologia da informação destinam-se a assegurar que as características de uma informação segura, confidencialidade (garantindo que o acesso aos dados apenas pode ser efectuado por pessoas autorizadas), integridade (garantindo que os dados não estão incompletos, não autorizados, etc), e disponibilidade (garantindo que os dados podem ser consultados, alterados, etc, a qualquer momento), estão presentes.

Como último tipo de controlo de supervisão surge então o controlo de utilizadores que respeita aos procedimentos tradicionalmente executadas manualmente sobre os documentos de transacções, tanto antes como depois do seu processamento informático, garantindo dessa forma um adequado e contínuo funcionamento dos diversos controlos das aplicações.

2.3.3. Risco de auditoria

O conceito de risco de auditoria permite ao auditor realizar uma auditoria de forma eficaz e eficiente (IFAC:NIR 300, 2004), podendo este basear a sua auditoria no modelo de risco de auditoria, sendo o modelo emanado pelo AICPA o mais amplamente aceite (Kinney, 1989). Para a prossecução do nosso estudo, entendemos então verificar qual o conceito de risco de auditoria a seguir. Como tal, e tendo em conta que o modelo de risco de auditoria preconizado pelo AICPA se encontra reflectido em normas nacionais, optamos por analisar a NIR nº 400 – Avaliações do risco e controlo interno.

Esta norma define risco de auditoria como sendo “o risco de o revisor/auditor dar uma opinião de revisão/auditoria inapropriada quando as demonstrações estejam

distorcidas de forma materialmente relevante" (OROC; DRA 400, ????). Dessa forma, o risco de auditoria é inversamente proporcional ao nível de segurança que o auditor se propõe atingir.

Verificamos ainda, pela leitura desta norma que o risco de auditoria pode ser dividido em três componentes: risco inerente, risco de controlo e risco de detecção, as quais interessa analisar separadamente, apresentando-se essa análise nos seguintes pontos.

Risco de Auditoria = Risco Inerente X Risco de Controlo X Risco de Detecção

2.3.3.1. O risco inerente

O risco inerente é a "susceptibilidade de um saldo de conta ou uma classe de transacções a uma distorção que possa ser materialmente relevante, individualmente ou quando agregada com distorções em outros saldos ou desses, assumindo que não existissem os respectivos controlos internos." (IFAC: NIR 300, 2004)

O risco inerente é independente do objectivo do auditor, não sendo portanto possível a este alterar o nível de risco que corre. Terá, porém, na fase do planeamento, de o avaliar, tendo em conta o seu peso na fixação no risco de auditoria. Para efectuar a seu julgamento do nível de risco inerente, o auditor poderá socorrer-se da NIR nº 400, a qual elenca numerosos exemplos de factores de risco inerente, alguns dos quais, conforme veremos mais adiante, serão utilizados no questionário a efectuar.

Para além do preconizado pela NIR nº 400 referida acima, verificamos ainda, pela NIR nº 401 – A revisão/auditoria num ambiente de sistema de informação computorizado, que o facto de estarmos perante um ambiente de TI pode afectar a revisão/auditoria. Porém, o objectivo dessa mesma revisão/auditoria, emitir uma opinião quanto à apresentação da imagem verdadeira e apropriada da posição financeira da entidade auditada, não se pode alterar por esse facto.

2.3.3.2. Risco de controlo

O risco de controlo é "o risco de uma distorção, que pudesse ocorrer num saldo de conta ou numa classe de transacções e que pudesse ser materialmente relevante, individualmente, ou quando agregada com distorções ou outros saldos ou classes, não vir a ser evitada ou detectada e corrigida numa base regular pelos sistemas contabilísticos e de controlo financeiro." (IFAC: NIR 400, ????)

Tal como acontece com o risco inerente, este não pode ser modificado pelo auditor, dependendo esse exclusivamente do SCI presente na organização.

O facto deste risco não poder ser modificado pelo auditor, não invalida porém que este deva ser avaliado pelo auditor na fase do planeamento de auditoria de forma a permitir a fixação do nível de risco de auditoria que este irá assumir. Dessa forma, o auditor procede à avaliação do risco de controlo de uma forma independente para as diversas rubricas que integram a informação financeira sobre a qual este vai emitir a sua opinião.

Com vista à formação do seu julgamento no que respeita ao risco de controlo, o auditor poderá socorrer-se de diversas técnicas, designadamente as enumeradas pela NIR nº 400: descrições narrativas, questionários, listas de verificação, fluxogramas, etc. Os testes de controlo que o auditor efectuará terão uma progressão inversa à do nível do risco de controlo fixado, ou seja, quanto maior o nível de risco de controlo que o auditor se propõe assumir, menor serão os testes de controlo e efectuar e inversamente no caso do auditor se propor assumir um risco de controlo baixo. Os testes de controlo efectuados permitirão dessa forma validar o julgamento do auditor quanto ao nível de risco de controlo fixado.

2.3.3.3. Risco de detecção

O risco de detecção é "o risco de os procedimentos substantivos do revisor/auditor não virem a detectar uma distorção que possa ser materialmente relevante, individualmente ou quando agregada com distorções ou outros saldos de classes." (IFAC: NIR 400, ????)

Este risco é o único que o auditor pode influenciar, visto que depende directamente do trabalho deste, o qual é influenciado pelo seu julgamento no que respeita aos riscos inerente e de controlo. Dessa forma, ao auditor poderá efectuar o seu planeamento no que respeita aos testes substantivos a efectuar, os quais deverão servir de suporte à sua opinião.

Pelo facto do risco de detecção ser fixado tendo em conta os riscos inerente e de controlo, temos que este é o inverso desses dois riscos. Por isso, quando o auditor avaliar um risco, combinado, inerente e de controlo, alto, deverá fixar um risco de detecção baixo, levando a uma maior realização de testes substantivos. Porém, fixando-se um nível combinado de risco inerente e de controlo baixo, então poderá fixar-se um nível de detecção alto, levando a que os testes substantivos efectuados sejam reduzidos.

Alterando a fórmula apresentada, anteriormente, do risco de auditoria, temos então que:

$$\text{Risco de detecção} = \frac{\text{Risco de auditoria}}{\text{Risco inerente X Risco de controlo}}$$

A NIR 400 apresenta, ainda, no seu apêndice, o seguinte quadro para avaliação do risco de detecção mostrando a relação existente entre as três componentes do risco de auditoria, sendo evidenciado a sombreado a influência do risco inerente e do risco de controlo no risco de detecção, conforme segue:

		Avaliação pelo revisor/auditor do risco de controlo		
		Alto	Médio	Baixo
Avaliação pelo revisor/auditor do risco inerente	Alto	O mais baixo	Mais baixo	Médio
	Médio	Mais baixo	Médio	Mais Alto
	Baixo	Médio	Mais alto	O mais alto

2.3.4. Outsourcing

O desenvolvimento verificado nos últimos anos no que concerne aos meios de comunicação, designadamente a banalização da *Internet*, levou a que grande parte das organizações recorra actualmente ao *outsourcing* de parte das suas tarefas, em alguns casos fora do próprio território nacional. De entre essas tarefas, evidenciamos as relacionadas

com tecnologias de informação que produzem dados que servirão de base à organização para relatar a sua informação financeira.

O *outsourcing* corresponde genericamente à transferência de tarefas que anteriormente eram desempenhadas no seio da própria organização para uma entidade externa. Mas vejamos de forma mais pormenorizada algumas das definições dadas para *outsourcing*. O AICPA define que "o *outsourcing* significa contratar fornecedores independentes para satisfazer as necessidades internas", definindo ainda que "na indústria de SI, o *outsourcing* significa a utilização de entidades externas para fornecer serviços relacionados com informação (como o processamento, a gestão ou a manutenção de dados internos)". Para Antonucci, "O *outsourcing* de TI é genericamente definido como a contratação de fornecedores externos para desempenhar variadas funções de TI como: entrada de dados, operações de centro de dados, desenvolvimento e manutenção de aplicações, recuperação de desastre e gestão de redes de dados e operações". Como exemplo das situações descritas por Antonucci, para ajudar à compreensão, podemos imaginar uma organização cujo sistema de facturação dependa de uma entidade externa tendo a organização apenas de fornecer os dados de facturação, sendo estes posteriormente tratados pelo fornecedor de *outsourcing*, com impacto nos valores de volume de negócios, stocks, saldos de clientes, etc.

Constatamos ainda a existência de diversos tipos de *outsourcing*, podendo ser definidos em função de aspectos meramente quantitativos, aspectos económicos e contratuais, razões que levaram ao *outsourcing*, aspectos financeiros, e, por último, uma classificação global, mais abrangente, que abarca os diversos aspectos anteriormente focados.

2.3.4.1. Tipos de *outsourcing*

2.3.4.1.1. Divisão com enfoque na quantidade

Num aspecto meramente quantitativo existem dois tipos principais identificados designadamente, pelo AICPA, nomeadamente: total ou *outsourcing* puro (transferência da totalidade dos activos de SI para fornecedores de *outsourcing*) e selectivo

ou *outsourcing* híbrido. No caso do *outsourcing* selectivo existem várias formas de o definir, podendo ser considerado que estamos perante *outsourcing* selectivo ao tratar-se da transferência de apenas parte dos serviços de SI para o fornecedor externo ou podendo tratar-se de serviços de SI desenvolvidos em parceria entre os SI internos e o fornecedor externo.

2.3.4.1.2. Divisão com enfoque económico e contratual

Visto sob um aspecto económico e contratual, foram identificados por Thomsett três tipos de *outsourcing*, nomeadamente: global ou estratégico (transferência da totalidade de uma função de SI), não devendo ser confundido com o *outsourcing* total, visto estarmos a falar apenas de uma função e não da totalidade dos serviços de SI, *outsourcing* parcial ou táctico (transferência apenas de subfunções principais ou de projectos), e *outsourcing* de contratação ou alvo (transferência parcial de subfunções ou projectos).

2.3.4.1.3. Divisão com enfoque nos objectivos

Os objectivos que se pretendem atingir ao recorrer ao *outsourcing* levaram Lacity e Hirschheim à identificação de três tipos de *outsourcing*, nomeadamente: *outsourcing* total (transferência total para o fornecedor de uma parte significativa dos serviços de SI), gestão de projectos (transferência da realização de um projecto específico ou parte do trabalho de SI), e serviços pontuais ou *body shop* (transferência de serviços de SI de forma a satisfazer o aumento de procura a curto prazo).

2.3.4.1.4. Divisão com enfoque no aspecto financeiro

A classificação apresentada no ponto acima foi posteriormente revista revestindo um aspecto financeiro, entendendo Lacity e Hirschheim avaliar o tipo de *outsourcing* em função da percentagem do orçamento disponível para SI aplicada em *outsourcing*. Dessa forma surgiram então as classificações seguintes: *outsourcing* (transferência para os fornecedores de *outsourcing* de serviços despendendo pelo menos 80 % do orçamento disponível para SI), *insourcing* (transferência, após avaliação formal das várias propostas

apresentadas pelos fornecedores de *outsourcing* nos quais se incluem os departamentos internos da organização, de um máximo de 20 % do orçamento disponível para SI, mantendo-se dessa forma a restante percentagem do orçamento para aplicação interna), e *selective sourcing* (transferência para os fornecedores externos de 20 % a 60 % do orçamento total disponível para SI, sendo o restante orçamento aplicado internamente).

2.3.4.1.5. Divisão global

Para Millar, a identificação dos vários tipos de *outsourcing* existentes não pode ser vista sob formas tão restritivas, preferindo classificar os diversos tipos existentes através de uma conjugação dos aspectos focados nos parágrafos acima. Dessa forma, identifica quatro tipos de *outsourcing*, nomeadamente: *outsourcing* geral (*general outsourcing*), *outsourcing* transaccional (*transactional outsourcing*), *outsourcing* de processos de negócio (*business process outsourcing*), e *outsourcing* ligado a benefícios para o negócio (*business benefit outsourcing).* Analisemos de seguida estes tipos com mais pormenor.

O *outsourcing* geral pode, segundo Millar, revestir três formas diferentes: *outsourcing* selectivo ou *selective outsourcing* (transferência para os fornecedores externos de uma área particular da actividade de SI apenas), *outsourcing* de valor de acrescentado ou *value added outsourcing* (transferência para os fornecedores externos de uma área da actividade de SI para a qual, após análise, se considerou que os fornecedores externos poderiam acrescentar valor, sendo que a mesma actividade desenvolvida internamente não gera valor acrescentado de forma eficiente), e *outsourcing* cooperativo ou *cooperative outsourcing* (desenvolvimento de uma ou diversas actividades de SI em pareceria com os fornecedores externos).

O *outsourcing* transaccional corresponde a efectuar uma migração de uma plataforma tecnológica para outra, fornecida pela entidade externa, e é composto usualmente por três fases podendo qualquer uma delas ser transferida de forma independente para fornecedores externos, nomeadamente: gestão de sistemas ligados, transição para uma nova tecnologia, e estabilização e gestão de nova plataforma.

O *outsourcing* de processos de negócio, tipifica o contrato existente entre uma organização e um fornecedor externo em que este assume a totalidade responsabilidade pela realização de uma função do negócio inicialmente desenvolvida pela organização.

Por último, o *outsourcing* ligado a benefícios para o negócio, tipifica o contrato em que o fornecedor externo assume a partilha dos riscos e em que a sua remuneração pelo serviço é indexada aos benefícios proporcionados ao cliente para o seu negócio.

2.3.4.2. Riscos do *Outsourcing*

Face ao objectivo deste estudo interessa agora verificar quais os riscos incorridos pelas organizações que recorrem ao *outsourcing*. Os riscos incorridos com o recurso a fornecedores externos passam pelo facto da organização não controlar os aspectos externos, o que poderá comprometer a eficácia do seu controlo efectivo e afectar as características de informação segura que um SI deve possuir, confidencialidade, integridade e disponibilidade. Conclui-se que a análise do risco de recurso ao *outsourcing* passa pela análise dos factores externos que acabam por ter efeitos no ambiente externo à organização os quais, desde logo, esta não pode controlar. Estes factores constituem um risco incorrido com o processo de outsourcing por poderem afectar as características de informação segura. Esses factores são divididos em quatro grupos, nomeadamente: sociológicos, políticos e legais, económicos, e tecnológicos, mais frequentemente designados por factores PEST. Analisemos abaixo estes quatro factores com maior pormenor, salientando, desde já que os riscos desses factores externos poderem vir a afectar as características de informação segura serão, usualmente, mais importantes quando os fornecedores de *outsourcing* se situarem fora do território nacional em que se encontra a organização.

2.3.4.2.1. Factores sociológicos

Os factores sociológicos poderão existir tanto a nível interno como a nível externos. A nível interno, é sabido que será suficiente numa organização correr o rumor de que está a decorrer um eventual processo de *outsourcing* dos SI para que este influencie o ambiente que se vive na própria organização, podendo daí resultar riscos para os SI, ainda antes de se ter recorrido verdadeiramente ao *outsourcing*. Porém, mesmo depois de todo o processo de *outsourcing* concluído e devidamente implementado, o mesmo continua a ter uma influência sobre o ambiente vivido na organização, o qual poderá ter os mais variados

efeitos nesta. Um dos efeitos mais frequentemente verificado prende-se com a degradação da moral e da motivação das pessoas (PÀLVIA e al., 1995).

Para além dos factores sociológicos a nível interno, existirão os factores externos. Estes factores, podem situar-se ao nível interno dos fornecedores de *outsourcing* e do seu pessoal, mas também ao nível do ambiente em que este fornecedor se enquadra.

Ao nível do próprio fornecedor poderão surgir problemas que afectem a confidencialidade, a integridade, e a disponibilidade. Citando alguns exemplos podemos referir questões como o controlo do pessoal que integra a equipa do fornecedor, a integridade desse mesmo pessoal, o horário de funcionamento do fornecedor de outsourcing, etc. É importante que a organização que recorre ao *outsourcing* nunca esqueça que o fornecedor dirige ele próprio um negócio e tem, também ele, as suas motivações e objectivos para a gestão do seu negócio, os quais poderão nem sempre coincidir com as motivações e objectivos do cliente. Estes factores ainda serão, em nosso entender, passíveis de controlo pela organização, por meio de um contrato entre as duas entidades, organização e fornecedor, formulado cuidadosamente com o objectivo de minimizar a ocorrência de alguns destes factores ou, caso os mesmos ocorram, de minimizar os seus efeitos para a organização.

Referindo-nos agora ao ambiente externo em que o fornecedor se insere, evidenciamos questões relacionadas com cultura, religião, linguística, etc. Essas questões, acabam por influenciar o pessoal que integra a equipa do fornecedor, mas ainda o ambiente em que o mesmo se insere. Para esses factores não será possível, em nosso entender, à organização influenciar a sua ocorrência, podendo apenas tentar minimizar os seus efeitos. A ocorrência desses factores poderá ser essencialmente visível quando não existir correspondência entre o país em que a organização desenvolve o seu negócio e o país em que os fornecedores de *outsourcing* desenvolvem o seu.

2.3.4.2.2. Factores políticos e legais

Os factores políticos e legais incluem as acções derivadas do governo e que influenciam o ambiente externo em que se encontram inseridos os fornecedores de *outsourcing*. Estes factores têm uma grande influência sobre a forma como o negócio do fornecedor é gerido e, dessa forma, sobre os riscos para a organização que contrata os

serviços desses fornecedores. Em princípio, e tal como acontece com os factores sociológicos, a sua importância estará relacionada com a localização das empresas fornecedoras em relação à localização das organizações que a elas recorrem, porém, ao contrário do que acontecia com os factores sociológicos, os efeitos desses factores poderão fazer-se notar independentemente dos fornecedores se encontrarem no mesmo pais que a organização, já que poderão existir políticas divergentes de região para região. Podem ser referidos vários exemplos de factores de risco, designadamente: estabilidade do ambiente político, política económica seguida, legislação proteccionista, legislação laboral, etc.

Estes factores deverão ser analisados cuidadosamente pela organização antes de concluir o seu processo de outsourcing, visto, para esses não ser possível, em nosso entender, a organização influenciar a sua não ocorrência, podendo apenas tentar minimizar os seus efeitos.

2.3.4.2.3. Factores económicos

No caso dos factores económicos, as organizações devem ter em consideração os efeitos de uma economia de comércio, no curto e no longo prazo, especialmente quando se pretende agir no âmbito internacional. Nesse caso, a organização deverá ter em conta aspectos como as taxas de juros, os níveis de inflação, perspectivas da economia no longo prazo, etc.

2.3.4.2.4. Factores tecnológicos

Os factores tecnológicos podem ter uma influência vital para a vantagem competitiva da organização. Os factores tecnológicos levantam questões como as de saber se permitem que os produtos e os serviços sejam obtidos de forma mais económica, não comprometendo a qualidade e podendo mesmo esta vir a ser melhorada, independentemente do seu custo de produção. Será que ao recorrer a *outsourcing* a organização terá acesso a TI mais inovadoras ou obsoletas? Como pode o *outsourcing* de TI ser afectado pelos canais de distribuição informação? A tecnologia de distribuição da informação (ex: telefone, Internet, etc.) terá de ser avaliada de forma a identificar os eventuais factores de risco que daí poderão decorrer.

3. Estudo empírico

3.1. A forma de abordagem do problema

Face ao estudo realizado acima e tendo em conta os objectivos visados por este trabalho, concluir quanto ao impacto que o *outsourcing* de TI tem na avaliação que o auditor externo faz do risco de auditoria para a posterior emissão da sua opinião sobre o relato da administração no que respeita ao SCI inerente ao relato financeiro, será então realizado um estudo empírico.

Este estudo assenta numa hipótese geral, descrita no parágrafo anterior, e a qual será testada através de um questionário a efectuar aos ROC inscritos na OROC, e que tenham exercido a sua actividade com referência à data de 31 de Dezembro de 2005, por corresponder à data da última prestação de contas efectuada pelas empresas cujo exercício corresponde ao ano civil. Vejamos de seguida como desenvolver esse questionário.

O nosso questionário começará pela colocação de perguntas que deverão permitir a identificação do universo de respondentes quanto à sua experiência e como ROC e quanto à sua experiência quanto a empresas que integrem TI e quanto a empresas que recorrem ao *outsourcing* dessas TI. Estas perguntas poderão permitir estudar a existência de qualquer correlação entre as características do universo dos respondentes e os dados obtidos. Estas perguntas foram elaboradas de modo a possibilitar a obtenção de dados que poderão ser expressos em escala nominal com estudo de características dicotómicas (pergunta 1), ordinal (pergunta 2), e escala de rácios (perguntas 3 e 4). Face aos objectivos que se pretendem com estas perguntas entendemos que as mesmas não carecem de maior explicação nestes estudo, passando agora a evidenciar as restantes perguntas, salientando qual a razão da sua elaboração e a utilidade que avaliamos para as mesmas para o nosso estudo.

Para as restantes perguntas, a elaboração do nosso questionário teve em conta as questões levantadas no nosso estudo acima, e como tal seguiu a seguinte linha de

orientação: identificação do nível de SCI que os ROC avaliam como eficaz, verificação do julgamento dos ROC quanto à incidência que os factores PEST podem ter nas características da informação segura, e identificação de qual das duas componentes do risco de auditoria, não controlável pelo auditor, é afectada quando as características de informação segura são afectadas.

3.1.1. A avaliação do nível de SCI eficaz

A escolha desta pergunta resultou da análise da literatura em que verificamos que o auditor avaliará o julgamento inserido no relatório de SCI inerente ao relato financeiro, emitido pela administração, efectuando igualmente uma auditoria independente ao SCI inerente ao relato financeiro. Parece nos que apenas tendo o próprio auditor conhecimento do SCI inerente ao relato financeiro, e tendo ele efectuado os seus testes a este SCI estará em condições de se pronunciar sobre o relatório da administração. Para permitir a identificação do nível de SCI avaliado como eficaz optamos, conforme já tínhamos identificado em parágrafo acima, por seguir a linha de orientação do quadro conceptual do COSO. A nossa abordagem passou por não referir, de forma resumida os cinco níveis de SCI identificados pelo COSO, dando ao ROC apenas uma hipótese de resposta. Preferimos elencar um conjunto de características identificadas nesse quadro conceptual e referidas por alguns autores como essenciais no momento da revisão e efectuar ao SCI (ERNST & YOUNG, LLP, 2002; TORO, ????) , como necessárias para se concluir quanto ao nível de SCI da organização. Os ROC são então consultados no sentido de identificarem apenas 10 desses itens que considerem de maior relevância. Com este procedimento será possível recolher dados expressos qualitativamente em escala nominal. Dessa forma os ROC identificarão forçosamente itens correspondendo a vários níveis, permitindo-nos posteriormente fazer uma avaliação do nível de controlo elegido pelo ROC. Apresentamos de seguida uma relação das características a utilizar no nosso questionário, de acordo com a identificação do nível de SCI a que pertencem:

- Ambiente de controlo:
  - Integridade e valores éticos;

- Compromisso de competência profissional;
- Manual de políticas e práticas aplicadas aos recursos humanos.

- Avaliação de risco:
  - Política de gestão de risco;
  - Identificação dos riscos.

- Actividades de controlo:
  - Processos para evitar o acesso não autorizado;
  - Manual de procedimentos de informação;
  - Adequada segregação de funções;
  - Manual de políticas e procedimentos adoptados.

- Informação e comunicação:
  - Plano estratégico base (vinculado à estratégia geral da organização) para as TI;
  - Apoio da administração no desenvolvimento das TI (possibilitando nomeadamente recursos humanos e financeiros adequados);
  - Canais de comunicação que permitam a denúncia de eventuais factos não desejáveis;
  - Receptividade da direcção às sugestões dos empregados;
  - Canais de comunicação efectiva em toda a organização.

- Acompanhamento:
  - Concordância do pessoal em relação ao código de ética e conduta;
  - Auditoria interna efectiva;
  - Canais de comunicação ao pessoal sobre a evidência do bom funcionamento do SCI;
  - Metodologia lógica e adequada para avaliar o SCI;
  - Frequência e alcance de testes ao SCI adequados;
  - Mecanismos permitindo recolher e comunicar qualquer deficiência detectada no SCI;

- Acções de acompanhamento e melhoria contínua do SCI adequadas.

3.1.2. A avaliação da incidência de factores PEST

A escolha desta pergunta para o nosso questionário prendeu-se com o facto de termos verificado que os factores PEST são frequentemente associados a factores de risco decorrentes do *outsourcing* (SIEMS e al., 2003; VARAJÃO, 2001; CALDERON e al., 2004), sendo, ainda, alguns deles reconhecidos como factores de risco inerente ao nível das demonstrações financeiras, nomeadamente: factores económicos e factores tecnológicos (IFAC: NIR 400, ????). Nesta pergunta, avaliamos os efeitos destes factores nas características de informação segura, confidencialidade, integridade e, disponibilidade. Optamos por avaliar estes factores em função do seu efeito nessas características, visto que como verificamos no parágrafo 2.3.2. acima, estas características poderão ser afectadas se existir um deficiente controlo de TI.

Com vista à verificação do julgamento dos ROC quanto à incidência que os factores PEST podem ter nas características da informação segura optamos, por uma questão de consistência, por uma abordagem idêntica à seguida para a avaliação indicada no parágrafo acima, para o SCI. Como tal, optamos por não questionar de forma os ROC sobre a avaliação que fazem da incidência de factores PEST sobre as características da informação segura, preferindo apresentar uma relação de vários factores de risco PEST, retirados do nosso estudo à literatura existente sobre este assunto (VARAJÃO, 2001; CALDERON e al., 2004; REIBSTEIN, 1985).

A pergunta reveste porém uma forma ligeiramente diferente, destinando-se a recolher dados expressos de forma qualitativa, tem como base uma escala ordinal, utilizando uma escala de Likert. Dessa forma, os ROC são consultados no sentido de identificarem para cada um dos itens citados, correspondendo a exemplos de factores PEST, de que forma julgam que estes poderão vir a afectar as características de informação segura. Para essa avaliação, serão dadas, com base na escala de Likert, as seguintes hipótese, quanto aos efeitos das situações descritas:

- não afectam as características de informação segura;

- afectam pouco as características de informação segura;
- afectam moderadamente as características de informação segura;
- afectam muito as características de informação segura;
- afectam totalmente as características de informação segura;

Esta forma de avaliação deverá permitir evidenciar quais os factores PEST que terão mais impacto nas características da informação segura, e globalmente em que medida se pode considerar que esses factores afectam essas características.

Apresentamos de seguida uma relação dos factores PEST a utilizar para esta análise:

- Factores sociológicos:
  - Rumor de uma futura contratação de *outsourcing* para as TI (PÁLVIA e al., 1995);
  - Integridade do pessoal da equipa do fornecedor de *outsourcing* (VARAJÃO, 2001);
  - Horário de funcionamento do fornecedor de *outsourcing* (CALDERON, 2004).

- Factores políticos e legais:
  - Estabilidade do ambiente político (PUGH, 2006; MARKETING TEACHER, ????);
  - Política económica, financeira, laboral (PUGH, 2006; REIBSTEIN, 1985);
  - Existência de legislação proteccionista (CALDERON e al., 2004).

- Factores económicos:
  - Taxas de juro praticadas no país do fornecedor de *outsourcing* (PUGH, 2006);
  - Níveis de inflação no país do fornecedor de *outsourcing* (MARKETING TEACHER, ????, PUGH, 2006);

- Perspectivas da economia no longo prazo (MARKETING TEACHER, ????).

- Factores tecnológicos:
  - Tecnologia de distribuição da informação (MARKETING TEACHER, ????);
  - Existência de TI obsoletas (CALDERON e al., 2004);
  - TI não concebidas "à medida" para a organização (???, 2005; VARAJÃO, 2001).

3.1.3. A avaliação do risco de auditoria afectado

A identificação de qual das duas componentes do risco de auditoria, não controlável pelo auditor, é afectada quando as características de informação segura são afectadas terá interesse face à análise que efectuamos à literatura existente sobre o risco de auditoria.

Dessa revisão, concluímos que para duas das três componentes do risco de auditoria, nomeadamente risco inerente e risco de controlo o auditor não tem qualquer possibilidade de controlar o seu nível. Dessa forma, o risco de auditoria acabará por depender do risco de detecção que o auditor assumirá, sabendo que a sua avaliação corresponderá ao inverso da avaliação da conjugação do risco inerente e do risco de controlo, conforme vimos no ponto 2.3.3.3 acima. Sendo o risco de auditoria uma conjugação dessas três componentes, poderemos então concluir que, existindo uma variação na avaliação feita pelo auditor do risco de controlo, do risco de detecção, ou dos dois riscos simultaneamente, este terá de alterar o nível do risco de detecção que está disposto a correr com vista à fixação do risco de auditoria. Concluindo, assumindo um risco de detecção inicial médio, pressupondo que existem as características de informação segura, médio, poderemos verificar em que sentido o risco de detecção altera e, consequentemente, o risco de auditoria. Para uma avaliação futura dessa situação, propomos a utilização do seguinte gráfico, inspirado do modelo de fixação do risco de detecção, apresentado no ponto 2.3.3.3. acima, alterando este no sentido de representar as cinco categorias de avaliação previstas na escala de Likert.

Efeitos na avaliação do Risco inerente		Efeitos na avaliação do risco de controlo				
Aumento (+)	Total	----	---	--	-	=
	Moderado	---	--	-	=	+
	Nulo	--	-	=	+	++
	Moderado	-	=	+	++	+++
	Total	=	+	++	+++	++++
Diminuição (-)		Total	Moderado	Nulo	Moderado	Total
	Aumento (+)					Diminuição (-)

Com base neste gráfico, concluímos que para o caso em que o auditor julgue que o risco de controlo aumenta totalmente diminuindo simultaneamente o risco inerente totalmente, registaremos o aumento máximo do nível de risco de detecção fixado pelo auditor. Inversamente, se o risco de controlo diminuir totalmente aumentando simultaneamente o risco inerente totalmente, então registaremos a diminuição máxima do nível de risco de detecção fixado pelo auditor.

Com base neste quadro, avaliaremos os efeitos no risco de detecção derivados das variações dos riscos inerente e de controlo e, desde logo, visto estas componentes estarem interligadas, os efeitos no risco de auditoria, caso o auditor não altere o seu julgamento do risco de detecção face às alterações verificadas para os riscos inerentes e de controlo.

3.2. Análise das respostas obtidas

O questionário realizado para este estudo, e que evidenciamos no ponto 7.1 deste trabalho, esteve presente no site da OROC a partir de dia 15 de Fevereiro de 2006, por um período de aproximadamente um mês, no seguinte endereço: http://www.oroc.pt/fotos/editor2/Questionario_%20Joao%20almeida.xls, não se tendo porém obtido qualquer resposta a esse por essa via, pelo que, para contornar essa situação, optou-se por se proceder ao envio deste directamente por correio electrónico aos ROC e SROC cujos endereços de correio electrónico constavam do site www.pai.pt, tendo-se procedido ao envio do questionário para 116 endereços, conjugando ROC e SROC. Em

seguimento a este procedimento foi obtido um total de 21 respostas, tendo estas sido consideradas todas validas para o estudo a realizar. Após o tratamento dessas respostas com recurso ao SPSS, obtivemos os resultados que evidenciamos de seguida e que, numa primeira fase iremos tratar sob a forma descritiva.

3.2.1. Análise descritiva

3.2.1.1. Exercício da actividade de ROC

Das 21 respostas obtidas verificamos, que em 17 casos os respondentes exerciam a função de ROC com referência a 31 de Dezembro de 2005, conforme se pode verificar no quadro nº 1 – Exercício da função de ROC, evidenciado no ponto 7.2.1.1., retirado do SPSS.

3.2.1.2. Anos de exercício da actividade de ROC

Das 21 respostas obtidas verificamos que a maioria dos respondentes, 9 casos, exerce a sua actividade num período compreendido entre os 5 e os 10 anos, representando praticamente 43 % do total das respostas obtidas. De salientar ainda que para 3 dos questionários recebidos, os ROC não identificaram a resposta a esta pergunta, representando cerca de 14 % do total das respostas obtidas. Apresentamos no ponto 7.2.1.2., o quadro nº 2 – Anos de exercício da função de ROC, retirado do SPSS evidenciando estes dados.

3.2.1.3. Importância das TI nas entidades auditadas

Ao analisar as 21 respostas obtidas, temos que considerar apenas 17 como válidas já que para as restantes os respondentes não indicaram qualquer repartição do peso das TI nas entidades auditadas. Como tal, verificamos que, para a maioria dos respondentes, em cerca de 38 % das entidades auditadas, os mesmos consideram que as TI têm uma representatividade média. De referir porém que, os mesmos respondentes consideram ainda que, em cerca de 23 % dessas mesmas entidades as TI estão fortemente representadas tendo os mesmos indicado a hipótese “TI com representatividade muito importante”,

contra menos de 2.5 % para a inexistência de qualquer representatividade das TI. Como conclusão, verificamos que em cerca de 38 % das entidades auditas as TI estão fortemente presentes, conforme se pode verificar no quadro nº 3 – Representatividade das TI nas entidades auditas, retirado do SPSS, apresentado no ponto 7.2.1.3.

3.2.1.4. Recurso a *outsourcing* de TI nas entidades auditadas

Da análise das 21 respostas obtidas a esta questão, concluímos ser de considerar apenas 17 como válidas já que para as restantes os respondentes não indicaram quantas das empresas auditadas recorriam a *outsourcing* para as suas TI. Esta questão permite verificar que a maioria das empresas auditadas pelos ROC (52 % das respostas consideradas válidas) não recorre ainda ao *outsourcing* das suas TI, sendo que apenas 47 % das entidades fazem *outsourcing* de TI. De salientar porém que embora a maioria não subcontrate as suas TI, a diferença entre as entidades que subcontratam e as que não subcontratam deve ser considerada mínima, evidenciando o que pensamos ser uma tendência no futuro de, cada vez mais, se subcontratar os mais variados serviços e não apenas os relacionados com TI. Evidenciamos no ponto 7.2.1.4 o quadro nº 4 – Quantidade de entidades auditadas que recorrem ao *outsourcing* de TI, retirado do SPSS para esse ponto.

3.2.1.5. Itens de maior relevância para concluir quanto à existência de SCI

A análise descritiva das 21 respostas obtidas para este ponto, evidenciada no ponto 7.2.1.5, no quadro nº 5 – Itens de maior relevância, permitiu concluir que todas como as respostas são válidas, tendo os respondentes respondidos correctamente em todos os casos.

Numa primeira análise descritiva, e visto a forma de estudo que optamos por seguir para esta questão, vamos verificar quais as principais três respostas obtidas. No sentido de justificar esta nossa opção, relembramos que as questões se encontram repartidas em cinco grupos distintos, correspondendo aos níveis de SCI evidenciados no quadro conceptual do COSO. Como tal, esperamos através desta análise poder tirar alguma conclusão sobre o nível mínimo de SCI a partir do qual os respondentes consideram que estão perante um SCI que pode ser considerado eficaz.

Pela análise do mapa verificamos que o item de maior relevância para os respondentes, nomeadamente, acções de acompanhamento e melhoria contínua do SCI adequadas, corresponde a um dos itens representativos do nível de acompanhamento. Porém, quando analisamos o segundo item de maior relevância, concluímos que o mesmo representa o primeiro nível de SCI previsto no quadro conceptual do COSO, ambiente de controlo. Esta resposta parece-nos surpreendente já que é o oposto do item de maior relevância deste questionário. Importa porém salientar a importância dada neste caso, pelos respondentes, à integridade e valores éticos.

Passando por estas duas aparentes contradições, a análise das respostas parece depois decorrer maioritariamente, conforme os níveis de SCI previstos pelo quadro conceptual do COSO, sendo que a evolução dos sete itens de maior relevância para os respondentes evolui, à excepção dos dois primeiros, conforme já referimos, conforme previsto pelo quadro conceptual do COSO. De salientar ainda que os respondentes não parecem atribuir grande relevância ao nível de informação e comunicação, penúltimo nível do quadro conceptual.

3.2.1.6. Situações que afectam as características de informação segura

A análise descritiva das 21 respostas obtidas para este ponto permitiu concluir que todas como as respostas são válidas, tendo os respondentes respondidos correctamente em todos os casos.

Numa primeira análise descritiva, e visto a forma de estudo que optamos por seguir para esta questão, vamos verificar quais as principais três respostas obtidas. No sentido de justificar esta nossa opção, relembramos que as questões se encontram repartidas em quatro grupos distintos, correspondendo aos factores PEST que identificamos. Como tal, esperamos através desta análise, poder tirar alguma conclusão sobre qual ou quais os factores PEST que podem contribuir para influenciar as característica de informação financeira segura. Verificamos que os três factores mais escolhidos (Existência de TI obsoletas, TI não concebidas “à medida”, e técnicas de distribuição de informação utilizadas) correspondem todos a factores tecnológicos, pelo que podemos afirmar que para a maioria dos respondentes os factores tecnológicos, são os mais importantes. Somos ainda

de opinião que se deve relembrar uma das observações verificada no ponto 3.2.1.5 acima, que evidenciava a importância atribuída pelos respondentes à integridade e valores éticos. Nesta análise dos factores PEST, também esta importância acabe por ressaltar visto que, depois dos factores tecnológicos surgem os factores sociológicos, sendo que o primeiro foi, também ele, representado pela integridade do pessoal da equipa do fornecedor de *outsourcing*. O ponto 7.2.1.6 evidencia o quadro nº6 – Situações que afectam as características de informação segura, retirado do SPSS em que a nossa opinião se apoia.

3.2.1.7. Efeitos no julgamento do RA

Conforme verificamos no quadro nº 7 abaixo, a análise descritiva das 21 respostas obtidas para este ponto permitiu concluir que todas como as respostas são válidas, tendo os respondentes respondidos correctamente em todos os casos. Este ponto será tratado de forma mais aprofundada nos testes de hipóteses seguintes.

3.2.2. O teste de hipóteses

3.2.2.1. Hipótese geral a testar

Conforme temos vindo a referir ao longo deste estudo, somos de opinião que o *outsourcing* de TI tem impacto na avaliação do risco de auditoria pelo auditor. Sendo esta portanto a hipótese geral que entendemos testar com este estudo. A forma de testar esta hipótese, como referimos nos parágrafos acima passa pelo estudo de diversas correlações que relataremos de seguida, relacionadas com o impacto dos factores PEST nas características de informação financeira segura e com o impacto na avaliação de duas das componentes do risco de auditoria (risco inerente e risco de controlo) da não validação de características de informação financeira segura. Como tal, teremos de fixar várias hipóteses que nos deverão permitir retirar essa conclusão. Os próximos capítulos apresentarão essas várias hipóteses.

3.2.2.2. O teste da hipótese geral – hipóteses operacionais

Como forma de testar a nossa hipótese geral, entendemos usar alguns dos factores PEST (12 factores), retirados da revisão que efectuamos à literatura existente, no sentido de questionar de que forma os auditores avaliam que estes podem influenciar as características de informação segura. Tentaremos então verificar qual a relevância que cada um desses factores terá na avaliação da influência que exercem sobre as características de informação segura. Em conclusão, podemos formular a seguinte hipótese:

Hipótese 1: os respondentes consideram que os factores PEST afectam pelo menos moderadamente as características de informação segura.

Seguidamente, verificaremos o impacto que a não validação de pelo menos uma das características de informação segura tem no julgamento do auditor em relação a duas componentes do risco de auditoria, formulando então as seguintes hipóteses:

Hipótese 2: os respondentes consideram que a não validação de pelo menos uma das características de informação segura aumentam, pelo menos moderadamente, o risco de controlo.

Hipótese 3: os respondentes consideram que a não validação de pelo menos uma das características de informação segura aumentam, pelo menos moderadamente, o risco inerente.

3.2.2.2.1 Hipótese 1

O teste da nossa primeira hipótese passa pela soma dos dozes factores PEST identificados pelos respondentes de forma a permitir criar uma variável latente que poderemos denominar de influência global dos factores PEST nas características de informação segura.

Tendo usado uma escala de ordem para medir a influência dos factores PEST teremos de verificar, num primeiro tempo, qual o comportamento da distribuição desses factores, avaliando a sua normalidade. Para esta análise, retiramos os quadros nº 8 a nº 10, evidenciados no ponto 7.2.2.2.1 deste trabalho.

A análise do quadro nº8 - descrição das variáveis independentes, permitiu verificar que os valores obtidos para a assimetria (0.501) e para a curtose (0.972) são sempre inferiores a duas vezes o valor do erro padrão, permitindo concluir que não existe um problema importante de assimetria nas distribuições a analisar.

Como resultado dessa análise, concluímos que, embora nenhuma das variáveis tenha uma distribuição perfeitamente normal, conforme se verifica ainda no quadro nº 9 - Teste de normalidade, podemos considerar, que cada uma delas tem uma distribuição suficientemente normais para poderem ser consideradas como variáveis medidas por escalas de avaliação. Dessa forma, podemos somar os valores das componentes de forma a criar a nossa variável global denominada influência global dos factores PEST nas características de informação segura.

Feita a transformação das variáveis em variável global, teremos de calcular o coeficiente de fiabilidade (α) desta variável. Com recurso ao SPSS, retiramos o quadro nº 10 - Coeficiente de fiabilidade (α). Analisado este quadro, concluímos que o valor (α) apresentado (0.7087), pode ser considerado como sendo razoável face à literatura existente (Hill e al., 2005).

De seguida, interessa avaliar o grau de correlação entre os diversos factores PEST, o qual foi analisado com base no quadro nº 11 – Matriz de correlação.

Uma primeira abordagem do quadro das correlações existentes entre os diversos factores PEST põe em evidência, de forma clara, as quatros componentes PEST. Verifica-se que, existem quatro grupos distintos e perfeitamente identificáveis em que existe correlação positiva entre eles, conforme se pode verificar nos quadros que evidenciamos abaixo, subdivisões do quadro geral apresentado em anexo.

Factores políticos e legais

	EstPolit	PolEcFi	Protecci
EstPolit	1.0000		
PolEcFi	0.7897	1.0000	
Protecci	0.1049	0.3599	1.0000

Factores económicos

	TxJuro	Inflação	PerspEco
TxJuro	1.0000		
Inflação	0.9500	1.0000	
PerspEco	0.6128	0.6387	1.0000

Factores sociológicos

	RumorOut	IntegOut	Horário
RumorOut	1.0000		
IntegOut	0.2075	1.0000	
Horário	0.3420	0.0993	1.0000

Factores tecnológicos

	TecDistr	TIObsole	TINaoAMed
TecDistr	1.0000		
TIObsole	0.5183	1.0000	
TINaoAMed	0.3305	0.8378	1.0000

Em cada um dos quadros acima, verificamos que as correlações são positivas, tendo valores significativos, o que indicia que as componentes estão correlacionadas em cada uma das componentes PEST. Porém, e porque assumem valores intermédios, podemos afirmar que cada uma delas se refere a diferentes formas de avaliar os factores PEST.

Passando à leitura do quadro global, deparamo-nos tanto com valores de correlação positivos como negativos. Procedendo ao estudo dessas duas tendências, somos de opinião que qualquer uma delas encontra justificação face à natureza das próprias componentes. No sentido de ajudar à compreensão optamos, tal como fizemos acima, por divulgar aqui dois quadros, subdivisão do quadro geral evidenciado em anexo.

Correlação positiva

	EstPolit	PolecFi
PerspEco	0.5123	0.5978

Este quadro mostra a correlação positiva existente entre uma componente correspondendo aos factores económicos e duas componentes correspondendo aos factores políticos e legais. Como se pode verificar existe uma correlação entre as perspectivas económicas e, tanto a estabilidade política como a política económica e financeira, elevada. O facto dessas correlações serem positivas significa que as duas variáveis se movem no mesmo sentido. Esta situação é uma situação perfeitamente admissível e esperada estando a falar de factores relacionados.

Correlação negativa

	TaxaJuro	Inflação	PerspEco
TIObsole	-0.3435	-0.4376	-0.3406

Este quadro mostra a correlação negativa existente entre uma componente correspondendo aos factores tecnológicos e três componentes correspondendo aos factores económicos. Como se pode verificar existe uma correlação entre o investimento tecnológico e a política económica e financeira. O facto de essas correlações serem negativas significa que as duas variáveis se movem em sentido inverso. Ou seja, para política económicos de aumento de taxas de juros, inflacionistas, etc., o investimento em TI será menor, para uma política económica mais favorável, existirá em princípio maior propensão para investimento em TI.

Esta situação é uma situação perfeitamente admissível e esperada estando a falar de factores relacionados.

Face às diversas análises que efectuamos acima e, ainda, aos valores de fiabilidade interna (α) (0.7087) que pode ser considerado razoável conforme referimos acima, concluímos que as componentes PEST apresentadas podem ser representadas como uma componente global e, por isso, concluímos que a hipótese é de aceitar. Afirmamos então que os factores PEST afectam, pelo menos moderadamente, as características de informação segura.

3.2.2.2.2 Hipótese 2

Para o teste desta hipótese interessa saber se a não validação de pelo menos uma das características de informação segura pode influenciar, pelo menos moderadamente, a avaliação que o auditor faz do risco de controlo, passando este a considerar que existe um aumento do risco de controlo nessa situação.

Tendo usado uma escala de ordem para medir a influência da não validação de uma característica de informação segura, teremos de verificar, num primeiro tempo, qual o comportamento da distribuição desses factores, avaliando a sua normalidade. Para esta análise, retiramos os quadros nº 12 a nº 14, evidenciados no ponto 7.2.2.2.2 deste trabalho.

A análise do quadro nº 12 - Descrição das variáveis independentes, permitiu verificar que os valores obtidos para a assimetria (0.501) e para a curtose (0.972) são inferiores a duas vezes o valor do erro padrão, permitindo concluir que não existe um problema importante de assimetria na distribuição a analisar.

Fazendo uma análise descritiva do comportamento das respostas obtidas, evidenciada no quadro nº 13 - Análise descritiva, verificamos que a média desta resposta se situa nos 4.0476, o que nos permite concluir que a não validação de pelo menos uma das características de informação segura afecta a avaliação que o auditor faz do risco de controlo, aumentando-o pelo menos moderadamente.

Estando a análise da normalidade da distribuição e ainda da influência da não validação de pelo menos uma das características da informação segura, e tendo em conta que estamos perante duas distribuições que podemos considerar relativamente normais podemos verificar qual o grau de correlação entre a nossa variável global (influência global

dos factores PEST nas características de informação segura) e a avaliação feita pelos auditores ao nível do risco de controlo. Para esse efeito, retiramos do SPSS o quadro nº 14 - Correlação entre influência global de factores PEST e Risco de controlo. Da análise deste quadro verificamos que existe uma muito ligeira correlação positiva entre estas duas variáveis, significando que as duas variáveis se movem no mesmo sentido, isto é quanto mais se considera que os factores PEST influenciam as características de informação segura, maior a avaliação do risco de controlo pelo auditor.

Das diversas análises que efectuamos acima concluímos que a não validação de pelo menos uma das características de informação segura, aumenta o julgamento que o auditor faz do risco de controlo, e que existe uma correlação entre os factores PEST, tomados como um todo e a avaliação feita pelo auditor do risco de controlo. Dessa forma, e tendo em conta a nossa opção de representar o *outsourcing* com o recurso aos factores PEST, concluímos que o recurso a *outsourcing* influência, embora de forma pouca significativa a avaliação que o auditor faz do risco de controlo.

3.2.2.2.3 Hipótese 3

Para o teste desta hipótese interessa saber se a não validação de pelo menos uma das características de informação segura pode influenciar, pelo menos moderadamente, a avaliação que o auditor faz do risco inerente, passando este a considerar que existe um aumento do risco inerente nessa situação.

Tendo usado uma escala de ordem para medir a influência da não validação de uma característica de informação segura, teremos de verificar, num primeiro tempo, qual o comportamento da distribuição desses factores, avaliando a sua normalidade. Para esta análise, retiramos os quadros nº 15 a nº 17, evidenciados no ponto 7.2.2.2.3 deste trabalho.

A análise do quadro nº 15 - Descrição das variáveis independentes, permitiu verificar que os valores obtidos para a assimetria (0.501) e para a curtose (0.972) são inferiores a duas vezes o valor do erro padrão, permitindo concluir que não existe um problema importante de assimetria na distribuição a analisar.

Fazendo uma análise descritiva do comportamento das respostas obtidas, evidenciada no quadro nº 16 - Análise descritiva, verificamos que a média desta resposta se

situa nos 3.3810, o que nos permite concluir que a não validação de pelo menos uma das características de informação segura afecta a avaliação que o auditor faz do risco inerente, aumentando-o pelo menos moderadamente.

Estando a análise da normalidade da distribuição e ainda da influência da não validação de pelo menos uma das características da informação segura, e tendo em conta que estamos perante duas distribuições que podemos considerar relativamente normais podemos verificar qual o grau de correlação entre a nossa variável global (influência global dos factores PEST nas características de informação segura) e a avaliação feita pelos auditores ao nível do risco inerente. Para esse efeito, retiramos do SPSS o quadro nº 17 - Correlação entre influência global de factores PEST e Risco inerente. Da análise deste quadro verificamos que existe uma muito ligeira correlação positiva entre estas duas variáveis, significando que as duas variáveis se movem no mesmo sentido, isto é quanto mais se considera que os factores PEST influenciam as características de informação segura, maior a avaliação do risco inerente pelo auditor.

Das diversas análises que efectuamos acima concluímos que a não validação de pelo menos uma das características de informação segura, aumenta o julgamento que o auditor faz do risco de controlo, e que existe uma correlação entre os factores PEST, tomados como um todo e a avaliação feito pelo auditor do risco inerente. Dessa forma, e tendo em conta a nossa opção de representar o *outsourcing* com o recurso aos factores PEST, concluímos que o recurso a *outsourcing* influência, embora de forma pouca significativa a avaliação que o auditor faz do risco inerente.

3.3. Conclusões a retirar do inquérito realizado

Face ao estudo das respostas obtidas ao questionário que efectuamos acima, e ainda ao objectivo que nos propomos atingir com este trabalho, podemos retirar várias conclusões.

Tendo o nosso estudo sido efectuado por meio da análise de três hipóteses, parece nos importante, relembrar as conclusões retiradas em cada uma dessas hipóteses numa primeira fase, articulando-as depois conjuntamente.

Para a primeira hipótese, influência dos factores PEST nas características de informação segura, concluímos que os factores PEST afectam pelo menos moderadamente as características de informação segura.

No segundo caso, influência da não validação de pelo menos uma das características de informação segura, na avaliação do risco de controlo, concluímos que essa não validação afecta, pelo menos moderadamente, a avaliação que o auditor faz do risco de controlo, considerando este que esse risco aumenta moderadamente.

Por último, na terceira hipótese, influência da não validação de pelo menos uma das características de informação segura, na avaliação do risco inerente, concluímos que a não validação afecta, pelo menos moderadamente, a avaliação do risco inerente feita pelo auditor, sendo que esse risco aumenta moderadamente quando uma das características de informação segura não é validada.

Conjugando as três conclusões acima, e porque seguimos a opção de avaliar os efeitos do *outsourcing* de TI na avaliação que o auditor faz do risco de auditoria através da influência de factores PEST nas características de informação segura, concluímos que se o os factores PEST influenciam as características de informação segura e se a não validação dessas características influenciam tanto o risco de controlo como o risco de auditoria, então o factores PEST influenciam o julgamento que o auditor faz dos riscos de controlo e inerente. Sendo o risco de auditoria composto por esses dois riscos, podemos então afirmar que os factores PEST e, consequentemente, o *outsourcing* influenciam o risco de auditoria, ainda que de forma moderada.

Não esquecendo o tema do nosso trabalho, temos de ter em atenção que a opinião do auditor referente ao julgamento que a administração inclui no relato financeiro sobre a eficácia do SCI presente na organização, deve ser apoiado sobre um correcto planeamento da auditoria a realizar de forma a proporcionar uma segurança razoável que o SCI inerente ao relato financeiro, é efectivo. Sabemos ainda que os auditores inquiridos, embora não tenham sido conclusivos quanto ao nível de SCI que se torna necessário atingir para que este se possa considerar efectivo, elegeram o nível de acompanhamento, último nível do quadro conceptual do COSO.

Como conclusão do acima referido, afirmamos que os auditores parecem muito exigentes quanto ao nível de SCI em que a organização se deve encontrar para que ele próprio possa considerar esse SCI efectivo, logo, terá de colocar um nível de risco de

auditoria baixo para avaliação do relato de controlo interno na administração. Para além disso, os auditores considerarem que os factores PEST influenciam esse mesmo risco de auditoria, aumentando o mesmo. Logo, o recurso a *outsourcing* de TI influenciará de forma importante o julgamento do risco de auditoria pelo auditor para efeitos de emissão de opinião sobre o relato do SCI inserido nas demonstrações financeiras.

4. Limitações e extensões

A realização deste trabalho ficou limitada em nosso entender essencialmente pela fraca adesão que tivemos ao nosso questionário, considerando que o número de respostas obtidas foi anormalmente baixo. Desconhecendo as razões dessas fraca adesão permitimo-nos porém opinar que as mesmas poderão estar relacionadas com o período em que o inquérito foi realizado, período tradicionalmente de muito trabalho para os auditores, com a forma de divulgação desse questionário, e ainda com algumas perguntas que eventualmente possam ter sido de compreensão mais difícil. Essas limitações poderão porém ser corrigidas num futuro trabalho, optando, para além da reformulação de algumas perguntas, pela adopção de outro período para a realização do questionário e ainda por outra forma de divulgação do mesmo, como era aliás nossa proposta.

Ao realizarmos este estudo, optamos por estudar os efeitos do *outsourcing* de TI na avaliação do risco de auditoria que o auditor está disposto a correr aquando da certificação do relatório sobre o SCI inerente ao relato financeiro. Este estudo poderia ser extensivo ao mesmo relatório, avaliando-se o risco de auditoria ao certificar o relato emitido pela administração sobre a eficácia do SCI inerente ao relato financeiro, não recorrendo a organização ao *outsourcing* das suas TI. Avaliando o efeito do *outsourcing* de TI, poderíamos avaliar futuramente o impacto deste, em cada uma das componentes do risco de auditoria tomadas separadamente, com base em cada uma das características da informação segura.

Por último, consideramos que este estudo poderia ser aprofundado, seguindo os mesmos objectivos, através do cruzamento de dados complementando os dados obtidos através do questionário aqui proposto com os dados obtidos através de um questionário a realizar a um universo de diversas organizações que recorram ao outsourcing de TI e que

sejam sujeitas a Revisão Legal das Contas. Este cruzamento poderia permitir evidenciar diferenças designadamente quanto ao nível de SCI considerado eficaz pelos relatores do SCI inerente ao relato financeiro e pelos indivíduos responsáveis pela certificação desse mesmo relatório.

5. Conclusões gerais do trabalho

Como conclusões deste trabalho, e tendo em conta algumas das limitações identificadas no parágrafo 5 acima, entendemos relatar os seguintes aspectos que nos pareceram de maior relevância ao longo deste estudo.

Relativamente ao panorama de auditoria, podemos afirmar que o mesmo sofreu uma alteração estando actualmente numa era que podemos designar de pós-Enron. Reflexo desta alteração foi o surgimento de diversa legislação, a nível internacional, que visa dar resposta aos problemas postos à luz do dia por esse e outros escândalos financeiros que lhe seguiram. Estes normativos vieram criar novas organismos normalizadores e, ainda, novas formas de relatórios, anteriormente não previstas. Como tal, a Administração passou a ter de relatar o SCI inerente ao relato financeiro e a ter de se pronunciar sobre a sua eficácia. Paralelamente, os auditores externos viram, também eles, alteradas as exigências que lhes são feitas, podendo-se nomear, entre outras, a de se pronunciarem sobre o dito relato da administração e sobre o próprio SCI inerente ao relato financeiro.

Como resultado dessas novas exigências, analisamos diversa literatura versando sobre estas matérias, tendo concluído que, muito embora não existam quaisquer exigências quanto ao normativo de controlo interno a utilizar para esta avaliação, podemos considerar que o COSO será um normativo adequado, passível de ser utilizado tanto pela administração das organizações aquando da preparação do seu relatório sobre o SCI inerente ao relato financeiro, como pelo auditor aquando dos testes que o mesmo realiza para formar a sua opinião sobre as asserções evidenciadas no citado relatório da administração.

Para além dos aspectos relacionados com o SCI inerente ao relato financeiro, foi possível verificar a opinião dos vários estudiosos destas matérias quanto ao facto das TI influenciarem os níveis de risco de auditoria que os auditores assumem. Verificou-se ainda

que estes níveis de risco poderiam ser ainda influenciados quando as empresas recorrem ao *outsourcing* para as suas TI. Concluindo-se, então, que o *outsourcing* de TI poderia ter um efeito maior na avaliação do risco de auditoria do que o efeito do simples recurso ao *outsourcing*, isto por força dos factores de risco PEST.

Falando na questão do *outsourcing* de TI, concluímos que parece haver uma grande diversidade de opiniões sobre quais os modelos de *outsourcing* que poderão existir, para além de, alguns autores, chegarem mesmo a divergir sobre o que se pode considerar *outsourcing*, tendo em conta as quantidades ou valores em que se recorre a um fornecedor externo para realizar determinado trabalho.

Este estudo permitiu-nos ainda concluir que os factores PEST influenciam as características de informação segura e que a não validação dessas características influenciam tanto o risco de controlo como o risco de auditoria. Como tal, concluímos que os factores PEST influenciam o julgamento que o auditor faz dos riscos de controlo e inerente. Face ao facto do risco de auditoria se compor por esses dois riscos, concluímos que os factores PEST e, consequentemente, o *outsourcing* influenciam moderadamente o risco de auditoria. Conjugando este estudo com o nosso trabalho, concluímos que o recurso a *outsourcing* de TI influenciará de forma importante o julgamento do risco de auditoria pelo auditor para efeitos de emissão de opinião sobre o relato do SCI inserido nas demonstrações financeiras.

6. Bibliografia

AICPA, *SAS nº 1 – Responsibilities and functions of the independent auditor*.

AICPA, 1998, Outsourcing Information Systems.

ANTONNUCCI, Y. L., LORDI, F. C., TUCKER III, 1998, *The pros and const of IT outsourcing – panacea or poison?*, Andersen Conulting.

CALDERON, Thomas G., CHANDRA, Akhilesh, 2004, *The impact of IT outsourcing on control risk*, Internal auditing, May/June, 23-30.

CANON, David M., GROWE, Glen A., 2004, *SOA Compliance: will IT sabotage your efforts?*, The journal of corporate & finance, July/August, 31-37.

CARNEIRO, Alberto, 2004, Auditoria de sistemas de informação, 2ª ed. aumentada, FCA – Editora de informática, Lisboa.

Deloitte & Touche LLP, Ernst & Young LLP, KPMG LLP, PricewaterhouseCoopers LLP, 2004, *Internal control over financial reporting – An investor resource*, December.

ERNST & YOUNG LLP, 2002, *Preparación de reportes sobre control interno – Una guía para la evaluación de la gerência conforme a la sección 404 de Sarbanes-Oxley Act*.

GUERINEL, Michèle Cartier le, LAYOT, Emmanuel, 2003, *Audit réalisé dans un milieu informatique*, http://www.crcc-paris.fr/docum/5a7_2003_paris.pdf, (10-10-04).

HASSID, Laurente, 2005, *LSF – SOA – Bale II: quelles obligations?*, http://www.itrmanager.com/39590-lsf,soa,bale,ii,obligations,laurent,hassid,bpms.html, (16-11-06).

HILL, Manuela Magalhães, HILL, Andrew, 2000, Investigação por questionário, 1º ed., Sílabo, Lisboa.

IFAC, NIR nº 300 – Planear uma auditoria de demonstrações financeiras.

___, NIR nº 400 – Avaliações do risco e controlo interno.

___, NIR nº 401 - A revisão/auditoria num ambiente de sistema de informação computorizados.

___, NIR nº 410 – Controlo interno.

___, RIPR nº 1001 – Ambiente de PED – Microcomputadores mono-posto.

___, RIPR nº 1002 – Ambiente de SIC – Sistemas de computador "em linha".

___, RIPR nº 1003 – Ambiente de TI – Sistemas de bases de dados.

___, RIPR nº 1008 – Avaliações do risco e controlo interno – Características e considerações de SIC.

___, RIPR nº 1009 – Técnicas de revisão/auditoria assistidas por computador.

ISACF, 2000(a), IT Governance Institute, Sponsors of CobiT, *CobiT – 3rd Edition - Executive summary*, July.

ISACF, 2000(b), IT Governance Institute, Sponsors of CobiT, *CobiT – 3rd Edition – Control objectives*, July.

ISACF, 2003, *IT control objectives for Sarbanes-Oxley*, www.deloitte.com/dtt/cda/doc/content/IT_Controls_%20Sarbanes-Oxley%281%29.pdf (23-03-05).

KINNEY, W. R. Jr., 1989, *Achieve audit risk and the audit outcome space*, *Auditing: a journal of practice and theory (supplement)*, 67-84.

LACITY, Mary Celia, HIRSCHHEIM, Rudy A., 1993, *Information systems outsourcing: myths, metaphors and realities*, 1º ed., John Willey & Sons, Inc., New York.

LACITY, Mary Celia, HIRSCHHEIM, Rudy A., 1995, *Beyond the information systems outsourcing bandwagon*, 1º ed., John Willey & Sons, Inc., New York.

LIJIMA, Timothy, CURTIS, Jeffrey, 2004, *Need to justify IT security? Measure your risk!*, *The journal of corporate & finance*, July/August, 47-51.

MARKETING TEACHER, ????, *PEST analysis. What is PEST analysis?*, http://marketingteacher.com/Lessons/lesson_PEST.htm (19-10-06).

McCONNELL JR, Donald K., ANKS, George Y., *How Sarbanes-Oxley will change the audit process*, http://www.aicpa.org/pubs/jofa/sep2003/mcconn.htm (12-10-04).

MILLAR, V., 1994, *Outsourcing trends*, *Proceedings of the cosourcing and insourcing conference*, University of California, Berkeley, November 4.

MOELLER, Robert, 2004, *Coping with SOX 404 requirements*, *The journal of corporate accounting & finance*, vol. 15, nº 6, September/October, 23-28.

NetMBA, ????, PEST Analysis, http://www.netmba.com/strategy/pest/ (04-12-06).

PÁLVIA, Prashant, PARZINGER, Monica, 1995, *Information systems outsourcing in financial institutions*, *Managing information technology investments with outsourcing*, Idea group publishing, 129-154.

PCAOB, *AS nº 2 – An audit of internal control over financial reporting performed in conjunction with an audit of financial statements.*

PUGH, Willis D., 2006, *One on one - An interview with, The journal of supply chain management, winter 2006*, 2-3.

RAMOS, Carla Margarida, PIMENTA, Carlos da Rocha, GONÇALVES, Dilene Vaz, 2001, A auditoria e as novas tecnologias de informação, *Revisores & empresas*, nº 11, Out/Dez, 11-20.

RAMOS, Michael, 2004, *Just how effective is your internal control?, The journal of corporate accounting & finance*, vol 15, nº 6, September/October, 29-33.

REIBSTEIN, David J., 1985, *Marketing – Concepts, strategies, and decisions*, 1º ed., Prentice Hall, Englewood Cliffs.

REIS, Elizabeth, MELO, Paulo, ANDRADE, Rosa, CALAPEZ, Teresa, 2003, Estatística aplicada – vol. 1, 4ª ed. Revista, Sílabo, Lisboa.

RESTEN, Alexandre, *L'audit des systémes d'information: une démarche intégrée à la mission permanente de commissariat aux comptes*, Thése professionnelle.

Sarbanes-Oxley Act, 2002, *Newsletter Revisores & Empresas*, nº 7, Dezembro, 1-7.

SGDM, *L'implication de la Loi nº 2003-706 du 1er août 2003 (dite Loi de Sécurité Financière) en Droit des sociétés*, http://www.afic.asso.fr/Images/Upload/DOCUMENTS/loi_securite_financiere_201003.pdf (16-11-06).

SIEMS, Thomas F., RATNER, Adam, S., *Beyond the border: do what you do best, outsource the rest*, http://www.dallasfed.org/research/swe/2003/swe0306c.html, (30-06-05).

SOUSA, Sérgio, 2003, Tecnologias de informação – o que são? Para que servem?, 4ª ed. Actualizada, FCA – Editora de informática, Lisboa.

THOMSETT, 1998, *Outsourcing: the great debate*, http://www.thomsettinternational.com/main/articles/hot/hot_outsource.htm (20-11-06).

TORO, Jorge Valência del, *Adoptando los modelos de control interno COSO y CoBIT*.

VARAJÃO, João Eduardo Quintela, 2001, *Outsourcing* de services de sistema de informação, 1º ed., FCA – Editora de informática, Lisboa.

107th CONGRESS, Senate and House of Representatives of the United States of America in Congress assembled, *The Sarbanes-Oxley Act of 2002*, Public Law 107-204.

???, 2005, Como garantir que a sua infra-estrutura de TI é gerida de uma forma segura – Realizar um *outrsourcing* em segurança, Contabilidade e empresas, Janeiro 2005, 13.

7. Anexos

7.1. Questionário

Questionário

(O tempo previsto para responder a este questionário é de aproximadamente 15 minutos)

1) Com referência a 31-12-05, exercia a sua actividade de Revisor Oficial de Contas (ROC)? (Assinalar com X)

Sim	
Não (passar ao ponto 5)	

2) Com referência a 31-12-05, há quantos anos exerce a sua actividade de ROC? (Assinalar com X)

Menos de 5 anos	
Entre 5 e 10 anos	
Entre 11 e 20 anos	
Mais de 21 anos	

3) Com referência a 31-12-05, proceda a uma repartição, **em percentagem**, das entidades que auditou quanto à importância (peso) que as tecnologias de Informação (TI) representam nas mesmas: (responder em percentagem)

TI sem qualquer representatividade	
TI com representatividade reduzida	
TI com representatividade média	
TI com representatividade importante	
TI com representatividade muito importante	
Não sabe	
Total	**0.00%**

4) Com referência a 31-12-05, proceda a uma repartição, **em percentagem**, das entidades que auditou, identificando quantas recorrem ao *outsourcing* das suas TI, independentemente da quantidade em que recorrem : (responder em percentagem)

Não recorrem ao *outsourcing*	
Recorrem ao *outsourcing*	
Não sabe	
Total	**0.00%**

5) Presupondo que, como auditor, validava a existência dos seguintes itens, assinale os 10 que considere mais relevantes para concluir quanto à eficácia do SCI presente na organização auditada. (Assinalar com X).

Integridade e valores éticos	
Compromisso de competência profissional	
Manual de políticas e práticas aplicadas aos recursos humanos	
Política de gestão de risco	
Identificação dos riscos	
Processos para evitar o acesso não autorizado	
Manual de procedimentos de informação	
Adequada segregação de funções	
Manual de políticas e procedimentos adoptados	
Plano estratégico base (vinculado à estratégia geral da organização) para as TI	
Apoio da administração no desenvolvimento das TI (possibilitando nomeadamente recursos humanos e financeiros	
Canais de comunicação que permitam a denúncia de eventuais factos não desejáveis	
Receptividade da direcção às sugestões dos seus empregados	
Canais de comunicação efectiva em todas a organização	
Concordância do pessoal em relação aos códigos de ética e conduta	
Auditoria interna efectiva	
Canais de comunicação ao pessoal sobre a evidência do bom funcionamento do SCI	
Metodologia lógica e adequada para avaliar o SCI	
Frequência e alcance de testes ao SCI adequados	
Mecanismos permitindo recolher e comunicar qualquer deficiência detectada no SCI	
Acções de acompanhamento e melhoria contínua do SCI adequadas	

6) Em que medida considera que as seguintes situações poderão afectar as caracteríticas de informação segura: confidencialidade, integridade, e disponbilidade? (Assinalar com X)

	Não afecta	Afecta pouco	Afecta moderadamente	Afecta muito	Afecta totalmente
Rumor de uma futura contratação de *outsourcing* para as TI	☐	☐	☐	☐	☐
Integridade do pessoal da equipa do fornecedor de *outsourcing*	☐	☐	☐	☐	☐
Horário de funcionamento do fornecedor de *outsourcing*	☐	☐	☐	☐	☐
Estabilidade do ambiente político	☐	☐	☐	☐	☐
Política económica, financeira, laboral.	☐	☐	☐	☐	☐
Existência de legislação proteccionista	☐	☐	☐	☐	☐
Taxas de juro praticadas no país do fornecedor de *outsourcing*	☐	☐	☐	☐	☐
Níveis de inflação no país do fornecedor de *outsourcing*	☐	☐	☐	☐	☐
Persectivas da economia no longo prazo	☐	☐	☐	☐	☐
Tecnologia de distribuição da informação (internet, etc)	☐	☐	☐	☐	☐
Existência de TI obsoletas	☐	☐	☐	☐	☐
TI não concebidas "à medida" para a organização	☐	☐	☐	☐	☐

7) Em que medida considera que a não validação de pelo menos uma das características de informação segura, evidenciadas na pergunta anterior, altera o seu julgamento dos seguintes itens: (Assinalar com X)

	Diminui totalmente	Diminui moderadamente	Mantem	Aumenta moderadamente	Aumenta totalmente
Risco de controlo	☐	☐	☐	☐	☐
Risco inerente	☐	☐	☐	☐	☐

8) Observações

Obrigado pela colaboração prestada

7.2. Relatórios SPSS

7.2.1. Análise descritiva

7.2.1.1. Exercício da função de ROC

Quadro 1 - Exercício da função de ROC

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Não exerceu a função de ROC	4	19.0	19.0	19.0
	Exerceu a função de ROC	17	81.0	81.0	100.0
	Total	21	100.0	100.0	

7.2.1.2. Anos de exercício da actividade

Quadro 2 - Anos de exercício da função de ROC

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Menos de 5 anos	2	9.5	11.1	11.1
	Entre 5 e 10 anos	9	42.9	50.0	61.1
	Entre 11 e 20 anos	4	19.0	22.2	83.3
	Mais de 21 anos	3	14.3	16.7	100.0
	Total	18	85.7	100.0	
Missing	-1.00	3	14.3		
Total		21	100.0		

7.2.1.3. Representatividade das TI

Quadro 3 – Representatividade das TI nas entidades auditadas

	N	Minimum	Maximum	Mean	Std. Deviation
TI sem representatividade	17	.00	20.00	2.3529	5.03663
TI com representatividade reduzida	17	.00	100.00	21.1765	25.46624
TI com representatividade média	17	.00	70.00	37.9412	24.81550
TI com representatividade importante	17	.00	35.00	14.4706	12.03182
TI com representatividade muito importante	17	.00	80.00	23.2353	25.05875
Não sabe / não se pronuncia	17	.00	.00	.0000	.00000
Valid N (listwise)	17				

7.2.1.4. Recurso a *outsourcing* de TI nas entidades auditadas

Quadro 4 - Quantidade de entidades auditadas que recorrem ao *outsourcing* de TI

	N	Minimum	Maximum	Mean	Std. Deviation
Não recorrem a outsourcing	17	.00	100.00	52.3529	36.66221
Recorrem a outsourcing	17	.00	90.00	47.0588	35.84074
Não sabe / não se pronuncia	17	.00	10.00	.5882	2.42536
Valid N (listwise)	17				

7.2.1.5. Itens de maior relevância para concluir quanto à existência de SCI

Quadro 5 - Itens de maior relevância

	N	Minimum	Maximum	Mean	Std. Deviation
Eficácia do SCI - Integridade e valores éticos	21	.00	1.00	.7143	.46291
Eficácia do SCI - Compromisso de competência profissional	21	.00	1.00	.5238	.51177
Eficácia do SCI - Manual de políticas e práticas aplicadas aos recursos humanos	21	.00	1.00	.2857	.46291
Eficácia do SCI - Política de gestão de risco	21	.00	1.00	.7143	.46291
Eficácia do SCI - Identificação dos riscos	21	.00	1.00	.7143	.46291
Eficácia do SCI - Processos para evitar o acesso não autorizado	21	.00	1.00	.6190	.49761
Eficácia do SCI - Manual de procedimentos de informação	21	.00	1.00	.1429	.35857
Eficácia do SCI - Adequada segregação de funções	21	.00	1.00	.7143	.46291
Eficácia do SCI - Manual de políticas e procedimentos adoptados	21	.00	1.00	.4762	.51177
Eficácia do SCI - Plano estratégico base	21	.00	1.00	.3810	.49761
Eficácia do SCI - Apoio da administração no desenvolvimento das TI	21	.00	1.00	.5238	.51177
Eficácia do SCI - Canais de comunicação para a denúncia de factos não desejáveis	21	.00	1.00	.3333	.48305
Eficácia do SCI - Receptividade da direcção às sugestões dos empregados	21	.00	1.00	.2857	.46291
Eficácia do SCI - Canais de comunicação efectiva em toda a entidade	21	.00	1.00	.5238	.51177
Eficácia do SCI - Concordância do pessoal em relação aos códigos de ética e de conduta	21	.00	1.00	.2381	.43644
Eficácia do SCI - Auditoria interna efectiva	21	.00	1.00	.4286	.50709
Eficácia do SCI - Canais de comunicaçao ao pessoal sobre a evidência do bom funcionaomento do SCI	21	.00	1.00	.1429	.35857
Eficácia do SCI - Metodologia lógica e adequada paa avalair o SCI	21	.00	1.00	.3810	.49761
Eficácia do SCI - Frequência e alcance de testes ao SCI adequados	21	.00	1.00	.4762	.51177
Eficácia do SCI - Mecanismos permitindo recolher e comunicar qualquer deficiência detectada no SCI	21	.00	1.00	.6190	.49761
Eficácia do SCI - Acções de acompanhamento e melhoria continua do SCI adequadas	21	.00	1.00	.7619	.43644
Valid N (listwise)	21				

7.2.1.6. Situações que afectam as características de informação segura

Quadro 6 - Situações que afectam as características da informação segura

	N	Minimum	Maximum	Mean	Std. Deviation
Rumor de uma futura contratação de outsourcing para as TI	21	1	5	2.62	1.071
Integridade do pessoal da equipa do fornecedor de outsourcing	21	2	5	3.57	1.028
Horário de funcionamento do fornecedor de ooutsourcing	21	1	4	2.71	1.189
Estabilidade do ambiente político	21	1	4	2.38	1.071
Política económica, financeira, laboral	21	1	4	2.62	1.244
Existência de legislação proteccionista	21	1	4	2.52	1.250
Taxas de juro praticadas no país do fornecedor de outsourcing	21	1	4	1.95	.921
Níveis de inflação no país do fornecedor de outsourcing	21	1	4	1.86	.964
Perspectivas da economia no longo prazo	21	1	4	2.48	.928
Tecnologia de distribuição da informação utilizada	21	2	5	3.81	.814
Existência de TI obsoletas	21	2	5	4.00	.949
TI não concebidas "à medida" para a organização	21	1	5	3.86	1.195
Valid N (listwise)	21				

7.2.1.7. Efeitos no julgamento do RA

Quadro 7 – Casos validos

	Cases					
	Included		Excluded		Total	
	N	Percent	N	Percent	N	Percent
Influência no risco de controlo da não validação de pelo menos uma das características de informação segura	21	100.0%	0	.0%	21	100.0%
Influência no risco inerente da não validação de pelo menos uma das características de informação segura	21	100.0%	0	.0%	21	100.0%

a Limited to first 100 cases.

7.2.2. Os testes de hipóteses

7.2.2.2. As hipóteses operacionais

7.2.2.2.1. Hipótese 1

Quadro 8 - Descrição das variáveis independentes

			Statistic	Std. Error
Rumor de uma futura contratação de outsourcing para as TI	Mean		2.62	.234
	95% Confidence Interval for Mean	Lower Bound	2.13	
		Upper Bound	3.11	
	5% Trimmed Mean		2.58	
	Median		3.00	
	Variance		1.148	
	Std. Deviation		1.071	
	Minimum		1	
	Maximum		5	
	Range		4	
	Interquartile Range		1.00	
	Skewness		.063	.501
	Kurtosis		-.037	.972
Integridade do pessoal da equipa do	Mean		3.57	.224
	95% Confidence	Lower Bound	3.10	

fornecedor de outsourcing	Interval for Mean	Upper Bound	4.04	
	5% Trimmed Mean		3.58	
	Median		4.00	
	Variance		1.057	
	Std. Deviation		1.028	
	Minimum		2	
	Maximum		5	
	Range		3	
	Interquartile Range		1.50	
	Skewness		-.517	.501
	Kurtosis		-.876	.972
Horário de funcionamento do fornecedor de ooutsourcing	Mean		2.71	.260
	95% Confidence Interval for Mean	Lower Bound	2.17	
		Upper Bound	3.26	
	5% Trimmed Mean		2.74	
	Median		3.00	
	Variance		1.414	
	Std. Deviation		1.189	
	Minimum		1	
	Maximum		4	
	Range		3	
	Interquartile Range		2.50	
	Skewness		-.370	.501
	Kurtosis		-1.377	.972
Estabilidade do ambiente político	Mean		2.38	.234
	95% Confidence Interval for Mean	Lower Bound	1.89	
		Upper Bound	2.87	
	5% Trimmed Mean		2.37	
	Median		2.00	
	Variance		1.148	
	Std. Deviation		1.071	
	Minimum		1	
	Maximum		4	
	Range		3	
	Interquartile Range		1.50	
	Skewness		.207	.501
	Kurtosis		-1.121	.972
Política económica, financeira, laboral	Mean		2.62	.271
	95% Confidence Interval for Mean	Lower Bound	2.05	
		Upper Bound	3.19	
	5% Trimmed Mean		2.63	
	Median		3.00	
	Variance		1.548	
	Std. Deviation		1.244	

	Minimum		1	
	Maximum		4	
	Range		3	
	Interquartile Range		3.00	
	Skewness		-.214	.501
	Kurtosis		-1.613	.972
Existência de legislação proteccionista	Mean		2.52	.273
	95% Confidence Interval for Mean	Lower Bound	1.95	
		Upper Bound	3.09	
	5% Trimmed Mean		2.53	
	Median		2.00	
	Variance		1.562	
	Std. Deviation		1.250	
	Minimum		1	
	Maximum		4	
	Range		3	
	Interquartile Range		3.00	
	Skewness		.025	.501
	Kurtosis		-1.678	.972
Taxas de juro praticadas no país do fornecedor de outsourcing	Mean		1.95	.201
	95% Confidence Interval for Mean	Lower Bound	1.53	
		Upper Bound	2.37	
	5% Trimmed Mean		1.89	
	Median		2.00	
	Variance		.848	
	Std. Deviation		.921	
	Minimum		1	
	Maximum		4	
	Range		3	
	Interquartile Range		2.00	
	Skewness		.526	.501
	Kurtosis		-.671	.972
Níveis de inflação no país do fornecedor de outsourcing	Mean		1.86	.210
	95% Confidence Interval for Mean	Lower Bound	1.42	
		Upper Bound	2.30	
	5% Trimmed Mean		1.79	
	Median		2.00	
	Variance		.929	
	Std. Deviation		.964	
	Minimum		1	
	Maximum		4	
	Range		3	
	Interquartile Range		2.00	
	Skewness		.681	.501
	Kurtosis		-.766	.972

Perspectivas da economia no longo prazo	Mean		2.48	.203
	95% Confidence Interval for Mean	Lower Bound	2.05	
		Upper Bound	2.90	
	5% Trimmed Mean		2.47	
	Median		3.00	
	Variance		.862	
	Std. Deviation		.928	
	Minimum		1	
	Maximum		4	
	Range		3	
	Interquartile Range		1.00	
	Skewness		-.338	.501
	Kurtosis		-.709	.972
Tecnologia de distribuição da informação utilizada	Mean		3.81	.178
	95% Confidence Interval for Mean	Lower Bound	3.44	
		Upper Bound	4.18	
	5% Trimmed Mean		3.84	
	Median		4.00	
	Variance		.662	
	Std. Deviation		.814	
	Minimum		2	
	Maximum		5	
	Range		3	
	Interquartile Range		1.00	
	Skewness		-.235	.501
	Kurtosis		-.218	.972
Existência de TI obsoletas	Mean		4.00	.207
	95% Confidence Interval for Mean	Lower Bound	3.57	
		Upper Bound	4.43	
	5% Trimmed Mean		4.06	
	Median		4.00	
	Variance		.900	
	Std. Deviation		.949	
	Minimum		2	
	Maximum		5	
	Range		3	
	Interquartile Range		1.50	
	Skewness		-.777	.501
	Kurtosis		-.006	.972
TI não concebidas "à medida" para a organização	Mean		3.86	.261
	95% Confidence Interval for Mean	Lower Bound	3.31	
		Upper Bound	4.40	
	5% Trimmed Mean		3.95	
	Median		4.00	

Variance	1.429	
Std. Deviation	1.195	
Minimum	1	
Maximum	5	
Range	4	
Interquartile Range	1.00	
Skewness	-1.447	.501
Kurtosis	1.653	.972

Quadro 9 - Teste de normalidade

	Kolmogorov-Smirnov(a)			Shapiro-Wilk		
	Statistic	Df	Sig.	Statistic	df	Sig.
Rumor de uma futura contratação de outsourcing para as TI	.258	21	.001	.887	21	.020
Integridade do pessoal da equipa do fornecedor de outsourcing	.328	21	.000	.810	21	.001
Horário de funcionamento do fornecedor de ooutsourcing	.214	21	.013	.831	21	.002
Estabilidade do ambiente político	.210	21	.016	.875	21	.012
Política económica, financeira, laboral	.200	21	.028	.821	21	.001
Existência de legislação proteccionista	.215	21	.013	.822	21	.001
Taxas de juro praticadas no país do fornecedor de outsourcing	.230	21	.005	.844	21	.003
Níveis de inflação no país do fornecedor de outsourcing	.289	21	.000	.803	21	.001
Perspectivas da economia no longo prazo	.285	21	.000	.857	21	.006
Tecnologia de distribuição da informação utilizada	.259	21	.001	.868	21	.009
Existência de TI obsoletas	.262	21	.001	.837	21	.003
TI não concebidas "à medida" para a organização	.357	21	.000	.755	21	.000

Quadro 10 - Coeficiente de fiabilidade alfa

Reliability Coefficients

N of Cases = 21.0 N of Items = 12

Alpha = 0.7087

Quadro 11 - Matriz de correlação

	RUMOROUT	INTEGOUT	HORARIO	ESTPOLIT	POLECFI	PROTECCI
RUMOROUT	1.0000					
INTEGOUT	0.2075	1.0000				
HORARIO	0.3420	0.0993	1.0000			
ESTPOLIT	0.3506	0.3372	0.5607	1.0000		
POLECFI	0.2608	0.4523	0.3621	0.7897	1.0000	
PROTECCI	-0.0302	0.1056	-0.2307	0.1049	0.3599	1.0000
TXJURO	-0.0700	0.1886	0.2610	0.4249	0.4199	0.3269
INFLACAO	-0.1038	0.1370	0.1371	0.4428	0.4528	0.3559
PERSPECO	0.1915	0.1721	0.4917	0.5123	0.5978	-0.0103
TECDISTR	-0.3169	0.4355	-0.2141	-0.4863	-0.3717	-0.0445
TIOBSOLE	-0.1476	0.4613	-0.0886	0.0492	0.1271	-0.1687
TINAOAME	-0.0446	0.4359	-0.0302	0.1618	0.3315	0.0861

	TXJURO	INFLACAO	PERSPECO	TECDISTR	TIOBSOLE	TINAOAME
PROTECCI	1.0000					
TXJURO	0.9500	1.0000				
INFLACAO	0.6128	0.6387	1.0000			
PERSPECO	-0.0795	-0.2278	-0.2711	1.0000		
TECDISTR	-0.3435	-0.4376	-0.3406	0.5183	1.0000	
TIOBSOLE	-0.1882	-0.2791	-0.2060	0.3305	0.8378	1.0000
TINAOAME						

8.2.2.2.2. Hipótese 2

Quadro 12 - Descrição das variáveis independentes

			Statistic	Std. Error
Influência no risco de controlo da não validação de pelo menos uma das características de informação segura	Mean		4.0476	.20090
	95% Confidence Interval for Mean	Lower Bound	3.6285	
		Upper Bound	4.4667	
	5% Trimmed Mean		4.1085	
	Median		4.0000	
	Variance		.848	
	Std. Deviation		.92066	
	Minimum		2.00	
	Maximum		5.00	
	Range		3.00	
	Interquartile Range		1.0000	
	Skewness		-.951	.501
	Kurtosis		.564	.972

Quadro 13 - Análise descritiva

	N	Minimum	Maximum	Mean	Std. Deviation
Influência no risco de controlo da não validação de pelo menos uma das características de informação segura	21	2.00	5.00	4.0476	.92066
Valid N (listwise)	21				

Quadro 14 - Correlação entre influência global factores PEST e Risco de Controlo

		Influência no risco de controlo da não validação de pelo menos uma das características de informação segura	Inflência global dos factores PEST
Influência no risco de controlo da não validação de pelo menos uma das características de informação segura	Pearson Correlation	1	.075
	Sig. (2-tailed)	.	.745
	N	21	21
Inflência global dos factores PEST	Pearson Correlation	.075	1
	Sig. (2-tailed)	.745	.
	N	21	21

7.2.2.2.3. Hipótese 3

Quadro 15 - Descrição das variáveis independentes

			Statistic	Std. Error
Influência no risco inerente da não validação de pelo menos uma das características de informação segura	Mean		3.3810	.17561
	95% Confidence Interval for Mean	Lower Bound	3.0146	
		Upper Bound	3.7473	
	5% Trimmed Mean		3.4233	
	Median		4.0000	
	Variance		.648	
	Std. Deviation		.80475	
	Minimum		2.00	
	Maximum		4.00	
	Range		2.00	
	Interquartile Range		1.0000	
	Skewness		-.844	.501
	Kurtosis		-.865	.972

Quadro 16 - Análise descritiva

	N	Minimum	Maximum	Mean	Std. Deviation
Influência no risco inerente da não validação de pelo menos uma das características de informação segura	21	2.00	4.00	3.3810	.80475
Valid N (listwise)	21				

Quadro 17 - Correlação entre influência global de factores PEST e Risco inerente

		Inflência global dos factores PEST	Influência no risco inerente da não validação de pelo menos uma das características de informação segura
Inflência global dos factores PEST	Pearson Correlation	1	.170
	Sig. (2-tailed)	.	.462
	N	21	21
Influência no risco inerente da não validação de pelo menos uma das características de informação segura	Pearson Correlation	.170	1
	Sig. (2-tailed)	.462	.
	N	21	21